uc3m | Universidad Carlos III de Madrid

Grado Universitario en Ingeniería Telemática
2017-2018

Trabajo Fin de Grado

"Cybersecurity Sorting Hat: Ampliación de funcionalidades de análisis y desarrollo de interfaz de usuario avanzada 1"

Sandra Sánchez Esperante

Tutora

Ana Isabel González-Tablas Ferreres

Madrid, 2018

RESUMEN

El presente documento tiene por objetivo detallar las funcionalidades del proyecto Cybersecurity Sorting Hat. Este proyecto es una aplicación web, inicialmente destinada a los alumnos del Máster de Ciberseguridad de la Universidad Carlos III, pero que puede ser modificada para ser de utilidad a todos los usuarios que quieran acceder a ella.

Originalmente el proyecto surgió de la necesidad de clasificar a los profesionales de la seguridad de la información en unos marcos muy definidos, por ello se tomó como referencia el marco más popular a nivel mundial conocido por NICE Cybersecurity Workforce Framework.

La principal funcionalidad de la aplicación es poder determinar el perfil, en términos de roles de ciberseguridad, de estos profesionales.

Este Trabajo Fin de Grado consiste en la continuación, modificación y mejora de un Trabajo Fin de Máster que realizó un compañero de la Universidad Carlos III.

El proyecto anterior ha tenido que ser rehecho desde cero en muchos aspectos como la interfaz de usuario o la estructura de código, también se han tenido que modificar bases de datos por lo que el diseño previo ha desempeñado un papel fundamental ya que ha tenido dos roles no solamente organizar las nuevas estructuras, sino que también ha sido vital para poder adaptar y modificar el Trabajo Fin de Máster.

Este documento detalla las etapas de planificación, diseño, desarrollo, y documentación que se han realizado durante el proyecto, asimismo explica las funcionalidades que se han desarrollado y la relevancia que tienen estas para el correcto funcionamiento de la aplicación.

PALABRAS CLAVE

· TFG: Trabajo Fin de Grado.

· TFM: Trabajo Fin de Máster.

· BOE: Agencia Estatal Boletín Oficial del Estado

· NICE: National Initiative for Cybersecurity Education.

· NIST: National Institute of Standards and Technology.

· NCWF: NICE Cybersecurity Workforce Framework.

· CSF: NIST Cybersecurity Framework.

· KSAs: Knowledge, Skills, and Abilities.

· TKSAs: Knowledges, Skills, Abilities and Tasks.

· IISP: Institute of Information Security Professionals.

· UX: User Experience.

· PHP: Hypertext Preprocessor.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ACLARACIONES PREVIAS SOBRE EL TRABAJO

Antes de comenzar con la lectura del proyecto, es necesario exponer los antecedentes de este. El Trabajo Fin de Grado es la continuación y mejora de un Trabajo Fin de Máster de un compañero del máster en Ciberseguridad de la Universidad Carlos III, Javier Vila, titulado "Cyber Range Systems: A Cybersecurity Sorting Hat".

Se trata de una aplicación web de gran dimensión que no podía ser completada en un único TFM, que se continúa y mejora en este Trabajo Fin de Grado.

El cliente tenía muchas ideas para completar este proyecto, y decidió distribuir las tareas en dos Trabajos de Fin de Grado paralelos, uno más centrado en el front-end y otro más centrado en el back-end. El primero es el que se presenta en esta memoria. El segundo lo finalizará posteriormente Javier Sanz López, un compañero de la Universidad.

Ambos hemos desarrollados distintas funcionalidades, pero compartimos el mismo núcleo y los Trabajos Fin de Grado se complementan mutuamente. Por tanto, esta complementariedad quedará reflejada en las memorias.

Inicialmente, ambos proyectos iban a ser presentados en la convocatoria de Junio de 2018, pero por motivos personales el Trabajo Fin de Grado de mi compañero se entregará en futuras convocatorias puesto que su parte está sin finalizar.

1. INTRODUCCIÓN

Este capítulo hace una breve introducción del proyecto y detalla la motivación que ha llevado a realizarlo. También se exponen los principales objetivos y funcionalidades que se van a desarrollar. Finalmente, se detalla la estructura que sigue el proyecto.

1.1. Motivación del Trabajo.

La sociedad actual es una sociedad hiperconectada. El internet de las cosas (IoT) ha facilitado la conexión de objetos que hace unos años no se hubiera podido imaginar que podrían acceder a internet.

Esta conexión de todo lo que nos rodea, desde la vida laboral a la personal, hace que sea necesaria la implantación de técnicas para proteger nuestra seguridad.

En 2017 vimos un aumento masivo de ciberataques [1], estos no solamente eran operaciones de ransomware contra empresas, sino que también hemos vivido ataques defendidos por estados, filtraciones de documentaciones estatales y hackeos de campañas electorales. Los más populares fueron la filtración Vault7 de Wikileaks y el ransomware WannaCry.

Solamente España registró el año pasado más de 120.000 ataques cibernéticos según INCIBE (Instituto Nacional de Ciberseguridad de España). Esta cifra ha aumentado un 140% en dos años [2].

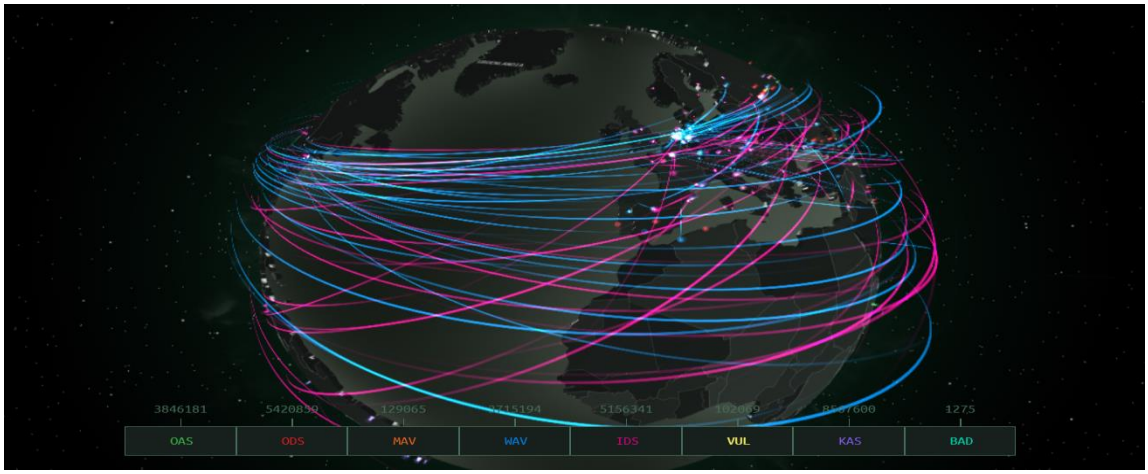


Figura 1.1. Captura que permite ver ciberamenazas en tiempo real [3]

Debido a este aumento masivo de ataques cada vez es más necesario la formación de profesionales en este sector. El Centro Mundial de Seguridad Cibernética y Educación (ISC) afirma en su Estudio Mundial de Seguridad de la Información (GISWS) que un 66% de empresas de seguridad no tienen suficientes empleados para hacer frente a todas las amenazas. Por lo que se prevé que los departamentos de seguridad se amplíen más de un 20% en el próximo año, lo que equivale a 1,8 millones de trabajadores más para cubrir esas vacantes [4].

Las empresas, con la esperanza de cubrir estas vacantes, buscan unos perfiles muy concretos. La finalidad de este proyecto es poder ayudar a los estudiantes a determinar qué perfil cumplen ó qué características o requisitos se buscan para un perfil concreto, y de esta manera poder aumentar sus ratios de empleabilidad. También es una herramienta útil para que las empresas puedan comprobar qué características deben cumplir sus empleados.

La clasificación de perfiles que vamos a seguir es la organización propuesta por NICE Cybersecurity Workforce Framework (NCWF) [5]. Esta clasificación se compone de 7 categorías que agrupan funciones comunes, 33 áreas de especialidad y 52 perfiles profesionales que a su vez comprenden los conocimientos y habilidades necesarios para desempeñar esos puestos.

1.2. Objetivos.

El Trabajo Fin de Grado pretende ayudar a profesionales del sector de la ciberseguridad descubrir cuál es su perfil y conocer qué aspectos de su carrera necesita mejorar para que puedan llegar a ser profesionales de éxito competitivos en el mercado laboral. Aunque los usuarios sean profesionales del sector IT, es importante desarrollar una aplicación sencilla y fácil de usar.

Teniendo en cuenta los requisitos podemos definir el objetivo principal como permitir al usuario descubrir su perfil en el sector de la seguridad informática y ofrecer herramientas para analizar dicho perfil. Es vital recordar que el TFM precursor a este proyecto intentó solventar esta necesidad, pero quedó incompleto y ha sido necesaria su

mejora y remodelación. Este TFG tiene por objetivos remodelar el front end y mejorar la seguridad de la aplicación web.

Para conseguir esto es necesario:

- Remodelar la estructura previa del proyecto anterior para optimizarla.
- Crear usuarios con sus procesos de autenticación para que la información sólo pueda ser visible por el propio usuario y de esta manera poder proteger la privacidad del usuario y su información confidencial.
- Diseñar una interfaz de usuario para que sea sencilla e intuitiva para los usuarios y sus respectivas pruebas de User Experience para comprobar que realmente se han cumplido estos objetivos.
- Rediseñar el conjunto de pantallas visibles para el usuario para poder aumentar las funcionalidades de la aplicación.
- Incluir dashboards con información del usuario para que pueda observar de una manera clara aquellas áreas que necesita reforzar.
- Incluir procesos seguros de autenticación contra la inyección SQL.

1.3. Estructura del documento.

Este apartado describe de manera general la estructura del documento.

- Introducción y objetivos: este capítulo trata la situación actual, el problema que existe en el sector de la ciberseguridad debido a la falta de perfiles profesionales y los numerosos ciberataques que se producen diariamente. Por tanto, se expone la necesidad de una aplicación que ayude a los profesionales a determinar su perfil y cuáles son sus debilidades y fortalezas.

- Estado de la cuestión: este capítulo se centra en revisar los aspectos técnicos de la situación actual. Se describen las aplicaciones similares que existen en otras naciones y se realiza una comparación de funcionalidades con la aplicación que se va a desarrollar en este Trabajo Fin de Grado. Asimismo, se exponen los marcos de perfiles de profesionales de ciberseguridad y cuáles son los motivos de la elección del NICE Cybersecurity Workforce Framework.

- Diseño y desarrollo software: estos capítulos analizan y describen el diseño de la solución técnica. Se detallan los desarrollos que se han realizado para conseguir una aplicación sencilla y útil. Trata todos los aspectos relativos a las modificaciones que se han desarrollado desde un punto de vista técnico.

- Planificación y presupuesto: este capítulo muestra la planificación previa que se ha realizado del proyecto. Asimismo, detalla la estimación de presupuesto del proyecto. Se trata de un capítulo importante puesto que muestra tanto la gestión de tiempo como de recursos.

- Marco regulador: se realiza un estudio de la legislación vigente española y europea que afectará a la publicación de la aplicación web.

- Conclusiones: este capítulo expone las conclusiones que se han extraído del Trabajo Fin de Grado. Se revisa el cumplimiento de los objetivos propuestos al principio del proyecto y se proponen futuras líneas de proyecto.

2. ESTADO DE LA CUESTIÓN

2.1. Situación actual.

La búsqueda de perfiles de ciberseguridad es una materia prioritaria en la actualidad para las empresas, por lo que podemos encontrar algunas páginas que realizan una función similar a la de este proyecto, pero ninguna es completamente igual.

Se ha realizado un análisis de la competencia actual para poder encontrar los aspectos diferenciales de nuestra aplicación, a continuación, se detallan las principales características de esta competencia. Debemos añadir que las aplicaciones mencionadas a continuación están orientadas a desarrollar la carrera profesional en Estados Unidos. Por lo tanto, podemos concluir en que no existe ninguna aplicación similar a la de este proyecto en el mercado.

2.1.1. National Initiative for Cybersecurity Careers and Studies (NICCS)

NICCS [6] es una aplicación web del gobierno estadounidense, perteneciente a Homeland Security, que conecta empleados gubernamentales, estudiantes y profesores con proveedores de capacitación de ciberseguridad.

La visión de NICCS es proporcionar las herramientas y los recursos necesarios para garantizar que los trabajadores en ciberseguridad tengan la capacitación y educación adecuadas. Su misión es ser un recurso para la educación, carreras y capacitación en ciberseguridad.

Estos cursos se desarrollan exclusivamente en Estados Unidos, en universidades norteamericanas y están destinados para ciudadanos estadounidenses. Al igual que en nuestro proyecto siguen la organización de The NICE Framework para categorizar los perfiles.

Además, podemos encontrar herramientas con funcionalidades similares a las que se van a desarrollar en este proyecto. Entre ellas podemos encontrar Mapping Tool y DHS PushButtonPD Tool.

Mapping Tool [7]: es una herramienta que permite a gerentes de seguridad y a profesionales del capital humano introducir información acerca de los puestos y comprobar si se alinean sus equipos con los establecidos en el Workforce Framework. En la actualidad, para acceder a esta funcionalidad es necesario ser un empleado de DHS (Department of Homeland Security)

DHS PushButtonPD Tool [8]: es un archivo de Excel sencillo y gratuito. Los gerentes y especialistas de recursos humanos pueden usar la herramienta para redactar rápidamente una descripción de la vacante federal sin la necesidad de una gran capacitación. El lenguaje que sigue es el definido por NICE (tareas, deberes y KSAs)

2.1.2 Cyberdegrees.org

CyberDegrees.org [9] fue creado por Degree Prospects, un editor de sitios web informativos en educación superior con sede en Washington.

Esta página tiene cuatro funcionalidades principales, las tres primeras denominadas "Degree Programs", "Online Degrees" y "Colleges by State" se centran en facilitar la información acerca de la educación en ciberseguridad. Todos estos cursos están asociados con universidades estadounidenses.

La cuarta funcionalidad es la que está relacionada con nuestro proyecto y que se denomina "Career Path". Al acceder podemos observar la siguiente pantalla:

Figura 2.1 Career Paths [9]

En esta sección podemos encontrar distintos puestos profesionales de la seguridad informática. Si hacemos clic en cada uno de ellos nos proporcionarán información como una breve descripción del puesto, las responsabilidades de este, otros puestos similares al que has seleccionado, salarios, habilidades necesarias para ser considerado para esa posición y finalmente certificaciones para esa función.

2.1.3 Institute of Information Security Professionals (IISP)

Se trata de un organismo independiente, sin fines de lucro, gobernado por sus miembros. Su sede se encuentra en Londres y fue creado en 2006 por profesionales del campo de la ciberseguridad [10].

Su página web ofrece una funcionalidad similar a la de este proyecto en la que el usuario puede comprobar que perfil de seguridad informática tiene, pero además podemos encontrar otras funcionalidades como la oferta de puestos de trabajos relacionados con perfiles en seguridad de la información.

Para poder acceder a sus servicios es necesario pagar una membresía. Dependiendo de ésta el usuario podrá acceder a un mayor número de funcionalidades.

Los distintos perfiles cumplen un marco diferente a las dos aplicaciones mencionadas anteriormente, no sigue el marco NCWF sino que toman como referencia un marco propio denominado IISP Skills Framework [11].

2.2. Marco actual.

Es importante exponer cuales han sido los motivos para escoger la clasificación propuesta NCWF y no otras categorizaciones existentes propuestas por otros organismos.

2.2.1. NICE Cybersecurity Workforce Framework (NCWF)

Es el marco más utilizado en la actualidad [5], es la base de la mayoría de las aplicaciones web descritas en el apartado anterior. Se trata de una publicación especial de NIST con alineación global que categoriza y describe los distintos puestos en ciberseguridad basados en TKSAs (Tasks, Knowledges, Skills, Abilities).

El marco NICE se compone de:

- 7 Categorías: agrupaciones de alto nivel de funciones comunes.
- 33 Área de especialidad: distintas áreas de trabajo.
- 52 Roles de trabajo: compuestos por TKSAs.

Figura 2.2. Las categorías del marco NICE Cybersecurity Workforce Framework [5]

El documento que recoge el marco, relaciona las categorías con las áreas de especialidad que le corresponden en tablas. A continuación, se muestra una tabla con un ejemplo de la relación entre ambas, traducida al castellano.

TABLA 2.1. NCWF SPECIALTY AREAS [12]

Categorías	**Área de especialidad**	**Descripción de Área de especialidad**
Investigar(IN)	Cyber Investigación (CI)	Aplica tácticas, técnicas y procedimientos para una gama completa de herramientas de investigación y procesos para incluir, entre otros, entrevistas e interrogatorios técnicas, vigilancia, contra-vigilancia y detección de vigilancia, y Equilibra de forma adecuada los beneficios de la persecución contra la recopilación de inteligencia.
	Forense Digital (FO)	Recopila, procesa, conserva, analiza y presenta evidencia relacionada con la computadora en apoyo de la mitigación de vulnerabilidad de red, y / o criminal, fraude, investigaciones de contrainteligencia o de aplicación de la ley

Adicionalmente, recoge tablas más completas que relacionan las categorías con las áreas de especialidad y grupos de trabajo, de estos últimos realiza una pequeña descripción. A continuación, se muestra un ejemplo:

TABLA 2.2. NCWF WORKROLES [12]

Categorías	**Áreas de especialidad**	**Grupos de trabajo**	**NCWF ID**	**Descripción de grupo de trabajo**
Investigar(IN)	Cyber Investigación (CI)	Investigador cibercrimen	IN-CI-001 I	Identifica, recopila, examina y preserva la evidencia utilizando análisis controlados y documentados y técnicas de investigación
	Forense Digital (FO)	Analista Forense	IN-FO-001	Lleva a cabo investigaciones profundas en computadora crímenes que establecen evidencia documental o física, a incluir medios digitales y registros asociados con cyber incidentes de intrusión
		Analista forense de ciberdefensa	IN-FO-002	Analiza la evidencia digital e investiga la computadora incidentes de seguridad para derivar información útil en apoyo de la mitigación de la vulnerabilidad del sistema / red.

Estos componentes serán los que vamos a usar en nuestra aplicación para determinar el grupo de trabajo al que van a pertenecer los usuarios y de esta manera proporcionarles información práctica sobre su perfil profesional. Todos los TKSA's del NCWF, se almacenarán en la base de datos de esta aplicación.

El documento recoge todos los TKSA's necesarios para un determinado perfil profesional en tablas como la que se muestra a continuación.

TABLA 2.3. NCWF WORKROLES DESCRIPTION [12]

ID Grupo de trabajo	SP-SYS-001
Categoría	Provisión segura (SP)
Área de especialidad	Desarrollo de sistemas (SYS)
Nombre del grupo de trabajo	Desarrollador de seguridad de sistemas de información (631)
Descripción del grupo de trabajo	Diseña, desarrolla, prueba y evalúa la seguridad del sistema de información a lo largo del ciclo de vida del desarrollo de sistemas.
Tasks	T0012, T0015, T0018, T0019, T0021, T0032, T0053, T0055, T0056, T0061, T0069, T0070, T0076, T0078, T0105, T0107, T0109, T0119, T0122, T0124, T0181, T0201, T0205, T0228, T0231, T0242, T0269, T0270, T0271, T0272, T0304, T0326, T0359, T0446, T0449, T0466, T0509, T0518, T0527, T0541, T0544
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0018, K0024, K0027, K0028, K0030, K0032, K0035, K0036, K0044, K0045, K0049, K0050, K0052, K0055, K0056, K0060, K0061, K0063, K0065, K0066, K0067, K0073, K0081, K0082, K0084, K0086, K0087, K0090, K0091, K0093, K0102, K0139, K0169, K0170, K0179, K0180, K0200, K0203, K0260, K0261, K0262, K0276, K0287, K0297, K0308, K0322, K0325, K0331, K0333, K0336
Skills	S0001, S0022, S0023, S0024, S0031, S0034, S0036, S0085, S0145, S0160
Abilities	[Sin especificar]

2.2.2. IISP Skills Framework

Propuesto por el IISP, este marco describe el rango de competencias que se espera de los profesionales de Seguridad de la Información para el correcto desempeño de sus tareas.

Fue desarrollado con la colaboración de organizaciones del sector público y privado, además de académicos y líderes de la seguridad de renombre mundial [10].

Posteriormente, se ha creado el IISP Knowledge Framework, que amplía el detalle de los conocimientos necesarios expuestos en el marco de este apartado [11].

2.2.3. U.S. Coast Guard Cybersecurity Framework Profile for Offshore Operations

Se trata de un marco definido por el departamento Offshore Operations the U.S. Coast Guard (USCG) del gobierno estadounidense en colaboración con National Institute of Standards and Technology (NIST) Cybersecurity Center of Excellence (NCCoE) [13].

Este marco orienta el marco NCWF a los campos de las misiones en el ejército estadounidense. Por lo tanto, es una adaptación del marco anterior al sector de la seguridad nacional.

A continuación, podemos observar un ejemplo de las subcategorías que este marco añade y la prioridad que tienen determinadas funciones.

Function	Category	Subcategory	Mission Objectives ●●● = High Priority, ●● = Moderate Priority, ● = Other Implemented Subcategories ✕ = Subcategories to NOT Implement											
			1	2	3	4	5	6	7	8	9	10	11	12
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	●●●	●●●	●●●	●●●	●	●	●	●●	●●	●	●	●●●
		ID.AM-2: Software platforms and applications within the organization are inventoried	●●●	●●●	●●	●●	●	●	●	●●	●	●	●	●
		ID.AM-3: Organizational communication and data flows are mapped	●●●	●●●	●	●	●	●	●	●	●●●	●	●●●	●●
		ID.AM-4: External information systems are catalogued	●●	●●	●	●●	●	●	●	●●	●●●	●	●●●	●
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and	●●●	●●●	●●●	●●●	●	●●●	●	●●●	●●●	●	●●●	●●●

Figura 2.3. Ejemplo de U.S. Coast Guard Cybersecurity Framework [13]

2.2.4. Financial Services Sector Specific Cybersecurity Profile ("Profile")

Al igual que el marco anterior se trata de un marco que nace a partir de una modificación del marco NCWF que incorpora aspectos de la regulación estadounidense. Está orientado a la seguridad de la información en sectores financieros [14].

Los cambios frente al marco del que parte son la adición de dos nuevas funciones a las previas que eran Identificar, Proteger, Detectar, Responder, Recuperar. Estas nuevas funciones son Gobernanza y Administración de dependencia.

Adicionalmente añade una nueva columna a las anteriores de Funciones, Categorías y Subcategorías denominada Posibles declaraciones de diagnósticos [15].

En la siguiente imagen podemos encontrar los cambios introducidos en este marco.

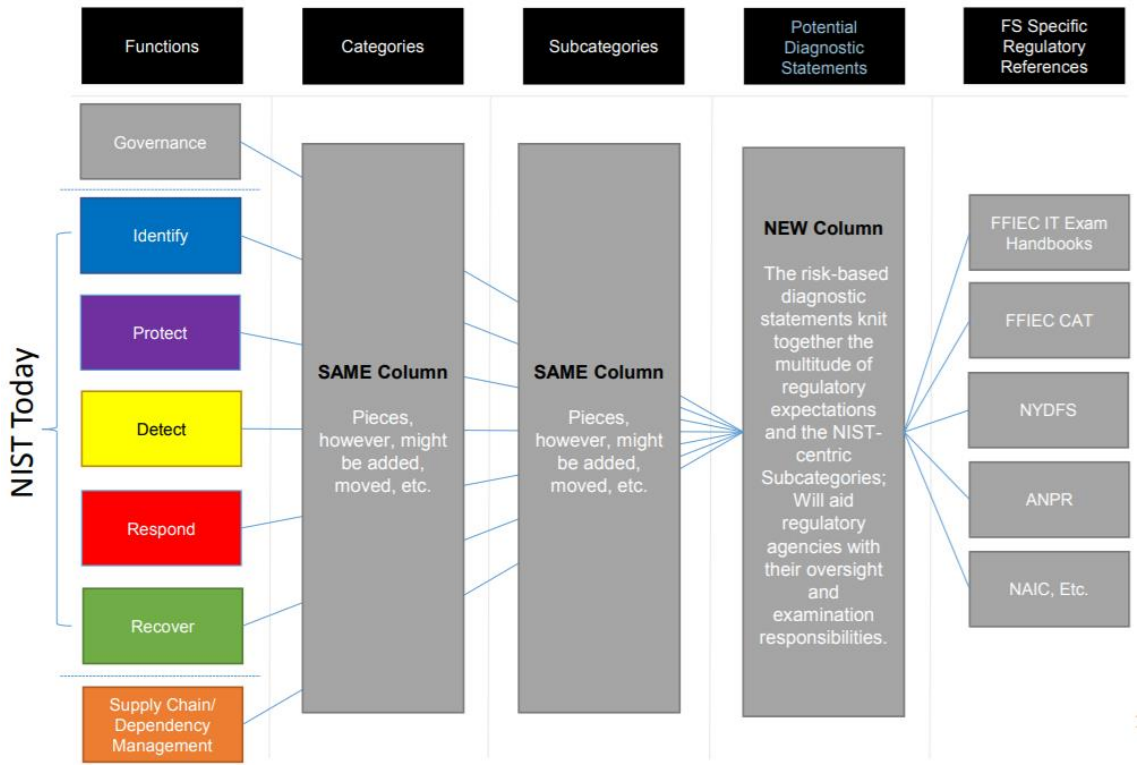


Figura 2.4. Cambios introducidos en este marco frente al marco NCWF [15]

2.3. Diseño de soluciones.

La solución propuesta para este proyecto consiste en el desarrollo de una aplicación web con funcionalidades únicas. Se trata de una aplicación puntera en el sector de la seguridad de la información y beneficiosa tanto para estudiantes como para empresas.

Esta solución, como hemos mencionado previamente, se basa en el marco NCWF. Hemos elegido este marco como la opción óptima ya que es la categorización de perfiles más común y popular en el sector de la ciberseguridad. Esta elección permite que el radio de usuarios sea mayor y que, a largo plazo, puedan usarla usuarios no pertenecientes únicamente a la Universidad Carlos III.

3. ANÁLISIS Y DISEÑO

En este capítulo se hace un análisis de la solución técnica y se describe la arquitectura que se propone para la aplicación. Posteriormente se exponen los requisitos del proyecto y los casos de uso.

3.1. Arquitectura de la aplicación

Para explicar de manera más sencilla la arquitectura de la aplicación, a continuación, podemos ver una figura con la división por capas.

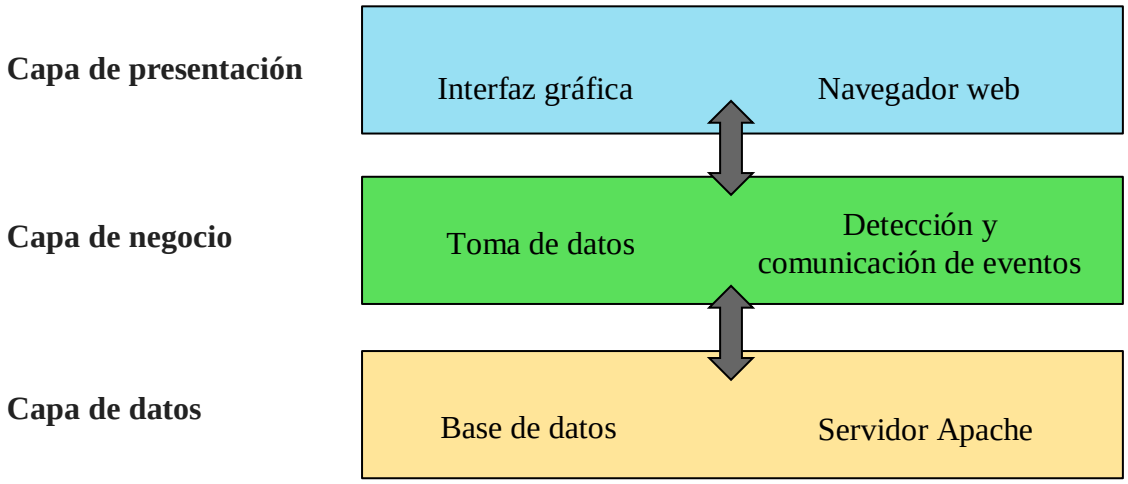


Figura 3.1. Arquitectura de la aplicación web

Se ha decidido representar las partes de la aplicación basándonos en la programación por capas, que se compone de tres capas [16].

La capa de presentación es aquella que ve el usuario, es la parte del sistema con la que interactúa. En nuestra aplicación se trata de la interfaz de usuario, es el medio con el que el usuario se conecta con el sistema. Este usuario accede a la interfaz gráfica mediante un navegador web. Podemos dividir esta capa de presentación a su vez en las cuatro vistas de la interfaz gráfica: pantalla de Login, pantalla de About, pantalla de Test y pantalla de Dashboard. Estas vistas serán explicadas en más detalle en el apartado 4 Desarrollo de software.

La capa de negocio es en la que residen los programas que se ejecutan, se reciben las peticiones del usuario y se envían las respuestas tras el proceso. En el caso de nuestra aplicación se trata del javascript que realiza las acciones que efectúan los usuarios en la interfaz gráfica. Entre las acciones que se encuentran en esta capa podemos encontrar registrar un usuario, iniciar sesión, hacer el test, procesar la información del test, crear el dashboard o cerrar sesión. Estas acciones serán detalladas más adelante en los casos de uso.

La capa de datos es donde residen los datos de la aplicación. Esta capa se compone en este proyecto de las bases de datos y el servidor Apache. La aplicación web consta de diversas bases de datos que no han sido desarrolladas en este proyecto, sino que fueron implementadas en los otros dos proyectos que comparten núcleo y nombre con este. Al tratarse de una aplicación realizada por varios desarrolladores sí que han sido usadas estas bases de datos en el proyecto.

El alcance de este proyecto comprende la realización desde cero de la capa de presentación. La mitad de la capa de negocio corresponde a la autora de este proyecto, concretamente, parte de la detección y comunicación de eventos y la otra mitad al autor del TFG con mismo nombre que este, Javier Sanz López. La capa de datos, como se ha mencionado previamente, fue realizada por el autor del TFM y primer desarrollador de este proyecto Javier Vila, aunque posteriormente ha sido retocado por Javier Sanz. Las partes desarrolladas en este proyecto serán explicadas más adelante.

3.2. Especificación de requisitos de software.

La especificación de requisitos de software (ERS) es una descripción del comportamiento ideal que debería tener el sistema que se va a desarrollar. [17] Podemos diferenciar entre requisitos funcionales y no funcionales.

3.2.1. Requisitos funcionales.

Son aquellos requisitos que equivalen a casos de uso.

TABLA 3.1. RF01 Registro de usuarios.

Identificador	RF01
Nombre	Registro de usuarios.
Descripción	El sistema proporcionará una pantalla con un formulario para que los usuarios puedan registrarse. El usuario introducirá sus datos para rellenar el formulario y enviará estos datos. El sistema deberá procesar estos datos correctamente y almacenarlos en la base de datos.
Requisitos previos	Ninguno.

TABLA 3.2. RF02 Autenticación de usuarios.

Identificador	RF02
Nombre	Autenticación de usuarios.
Descripción	El sistema proporcionará una pantalla con un formulario para que los usuarios puedan acceder a la plataforma. El usuario introducirá sus datos. El sistema deberá comparar estos datos con los que se encuentran en las bases de datos y comprobar si el usuario ha sido registrado.
Requisitos previos	Ninguno.

TABLA 3.3. RF03 Cierre de sesión.

Identificador	RF03
Nombre	Cierre de sesión.
Descripción	El sistema proporcionará un botón visible en todas las pantallas de la aplicación web que permita al usuario el cierre de sesión. El usuario accionará este botón. El sistema realizará el cierre de sesión y mostrará de nuevo la pantalla de login.
Requisitos previos	RF02.

TABLA 3.4. RF04 Cumplimentación del test.

Identificador	RF04
Nombre	Cumplimentación del test.
Descripción	El usuario accionará la pestaña en la que se encuentra el test. Rellenará los KSA's que correspondan con su perfil.
Requisitos previos	RF02

TABLA 3.5. RF05 Realización de test.

Identificador	RF05
Nombre	Realización de test.
Descripción	El usuario accionará el botón de realizar test. El sistema recogerá la información introducida por el usuario y la procesa.
Requisitos previos	RF02, RF04

TABLA 3.6. RF06 Modificación de test.

Identificador	RF06
Nombre	Modificación de test.
Descripción	El usuario podrá rehacer el test cuando desee. El usuario accionará el botón de realizar test. El sistema recogerá la información introducida por el usuario y la procesa.
Requisitos previos	RF02, RF04, RF05

TABLA 3.7. RF07 Consulta de dashboard.

Identificador	RF07
Nombre	Consulta de dashboard.
Descripción	El usuario accionará el botón de dashboard. El sistema mostrará los gráficos con la información del usuario.
Requisitos previos	RF02, RF04, RF05

3.2.2. Requisitos no funcionales.

Son aquellos requisitos que restringen el diseño o la implementación, en este tipo también podemos encontrar aquellos requisitos referentes a la calidad.

TABLA 3.8. RF08 Conexión a internet.

Identificador	RF08
Nombre	Conexión a internet.
Descripción	Será necesaria la conexión a internet para poder acceder a la aplicación. Asimismo, será necesaria la conexión durante toda la sesión.
Requisitos previos	Ninguno

TABLA 3.9. RF09 Protección de información.

Identificador	RF09
Nombre	Protección de información.
Descripción	Se garantiza la protección de la información de usuarios así como su confidencialidad.
Requisitos previos	Ninguno

TABLA 3.10. RF10 Desarrollo en PHP.

Identificador	RF10
Nombre	Desarrollo en PHP.
Descripción	El desarrollo de la aplicación se realizará en PHP manteniendo la decisión de lenguaje del proyecto anterior de Javier Vila.
Requisitos previos	Ninguno

3.3. Casos de uso.

Los casos de uso son las descripciones de las actividades que se deben realizar para llevar a cabo un proceso. Se trata de la secuencia de interacciones que se desarrollan entre un sistema y sus actores. [18]

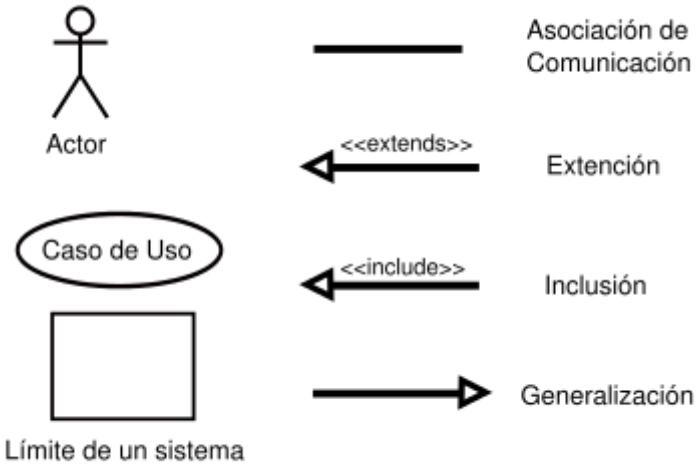


Figura 3.2. Notación de caso de uso [18]

Para realizar los casos de uso partiremos de los requisitos funcionales mencionados en el apartado anterior.

Registro de usuario

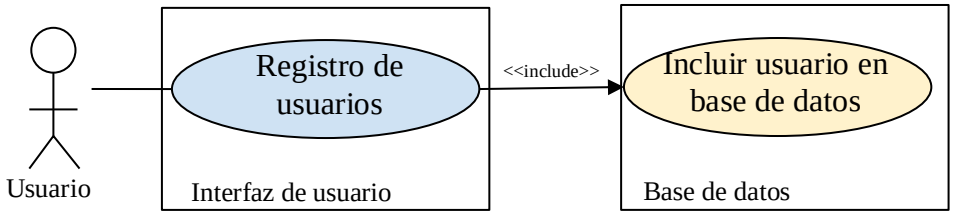


Figura 3.3. Caso de uso Registro de usuario.

Autenticación de usuario

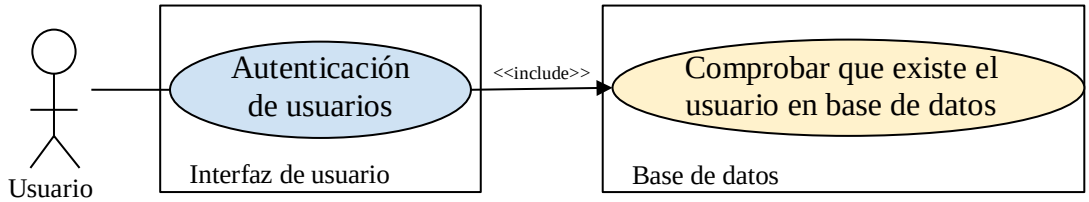


Figura 3.4. Caso de uso Autenticación de usuario.

Cierre de sesión

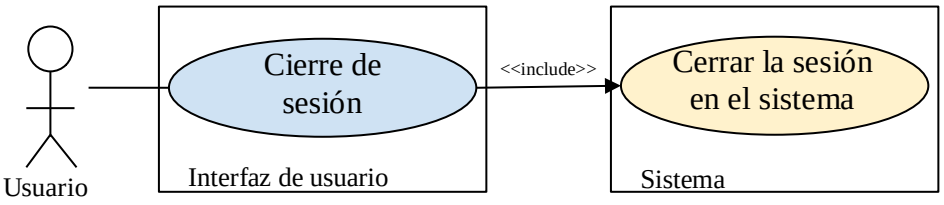


Figura 3.5. Caso de uso Cierre de sesión.

Cumplimentación el test

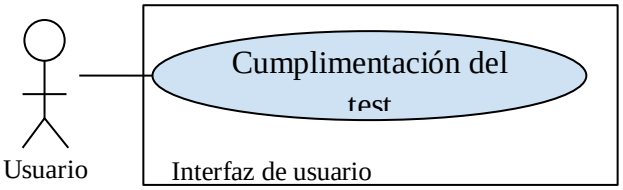


Figura 3.6. Caso de uso Cumplimentación de test.

Realización de test

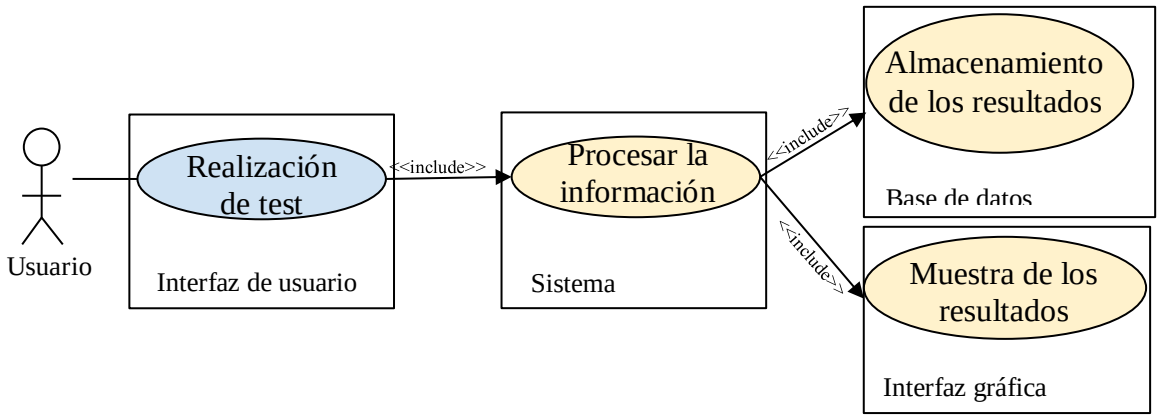


Figura 3.7. Caso de uso Realización de test.

Modificación de test

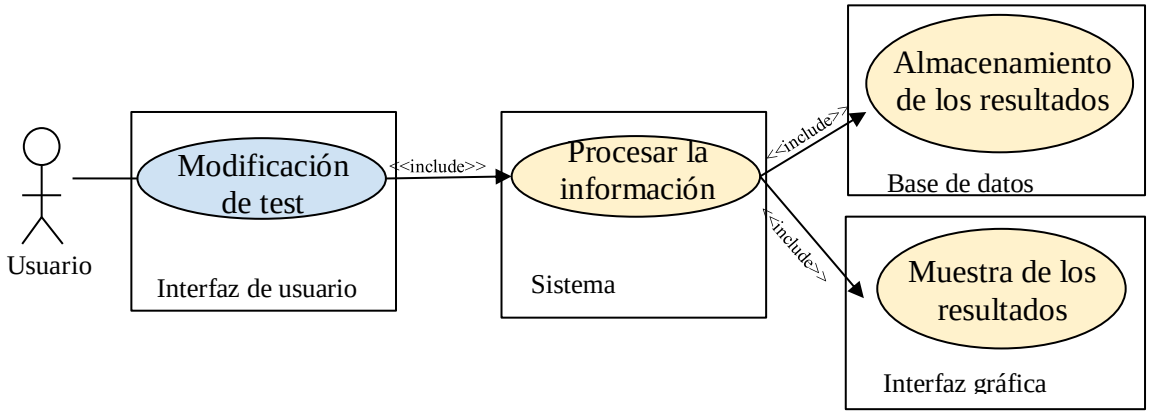


Figura 3.8. Caso de uso Modificación de test.

Consulta de dashboard

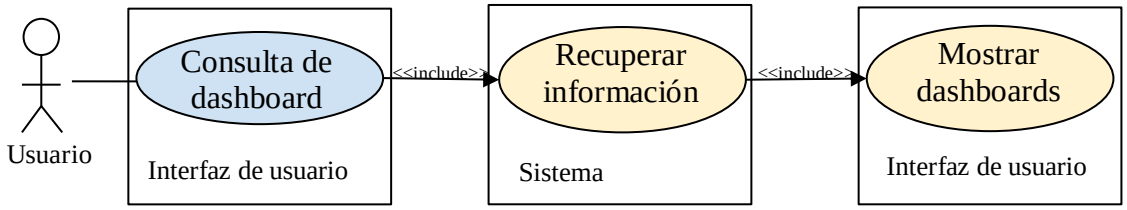


Figura 3.9. Caso de uso Consulta de dashboard.

4. DESARROLLO SOFTWARE

4.1. Diseño de la aplicación.

Este paso previo al desarrollo de la aplicación ha sido fundamental para llegar a la concordancia entre los requisitos y el resultado final del proyecto.

Este proyecto parte de un proyecto anterior, como se ha mencionado previamente, que no solamente ha sido necesario continuar, sino que han sido necesarias mejoras y modificaciones para optimizar la solución.

La aplicación ha sido desarrollada en HTML. Se ha mantenido el lenguaje de programación PHP en el que estaba desarrollada la versión anterior y que era utilizado para poder acceder a las bases de datos. PHP es un lenguaje de código abierto muy popular adecuado para el desarrollo web y que puede ser incrustado en HTML.

La aplicación se ha desarrollado en PHP, HTML, JS y CSS. Se ha utilizado PHP en lo relativo a la conexión con la base de datos y los intercambios de la aplicación con ella. HTML para realizar una aplicación web de manera estructurada. CSS se ha empleado para obtener una interfaz visualmente atractiva. JS para la detección y comunicación de eventos.

Se ha empleado una metodología “Agile” puesto que el proyecto precisaba de rapidez y era necesaria la colaboración entre dos alumnos de la universidad. Inicialmente se realizaron reuniones semanales para comprobar los avances del equipo y verificar que se estaban cumpliendo los objetivos, pero posteriormente, debido a motivos ajenos el compañero que realiza el Trabajo Fin de Grado que complementa a este tuvo que posponer su entrega y desarrollo de la aplicación.

Este Trabajo Fin de Grado ha tenido por objetivo realizar los requisitos que se plantearon al inicio y preparar un código estructurado y sencillo con la finalidad de facilitar la integración entre los códigos de dos desarrolladores cuando mi compañero complete sus requisitos.

Figura 4.1. Gráfico pasos metodología Agile [19]

4.2 Diagrama de flujo

A continuación, se encuentra el diagrama de flujo del proyecto completo, estos serán los pasos que deberá seguir el usuario cuando quiera utilizar la aplicación. Este diagrama no incluye el registro puesto que se ha representado en un diagrama de flujo separado y que podremos observar más adelante.

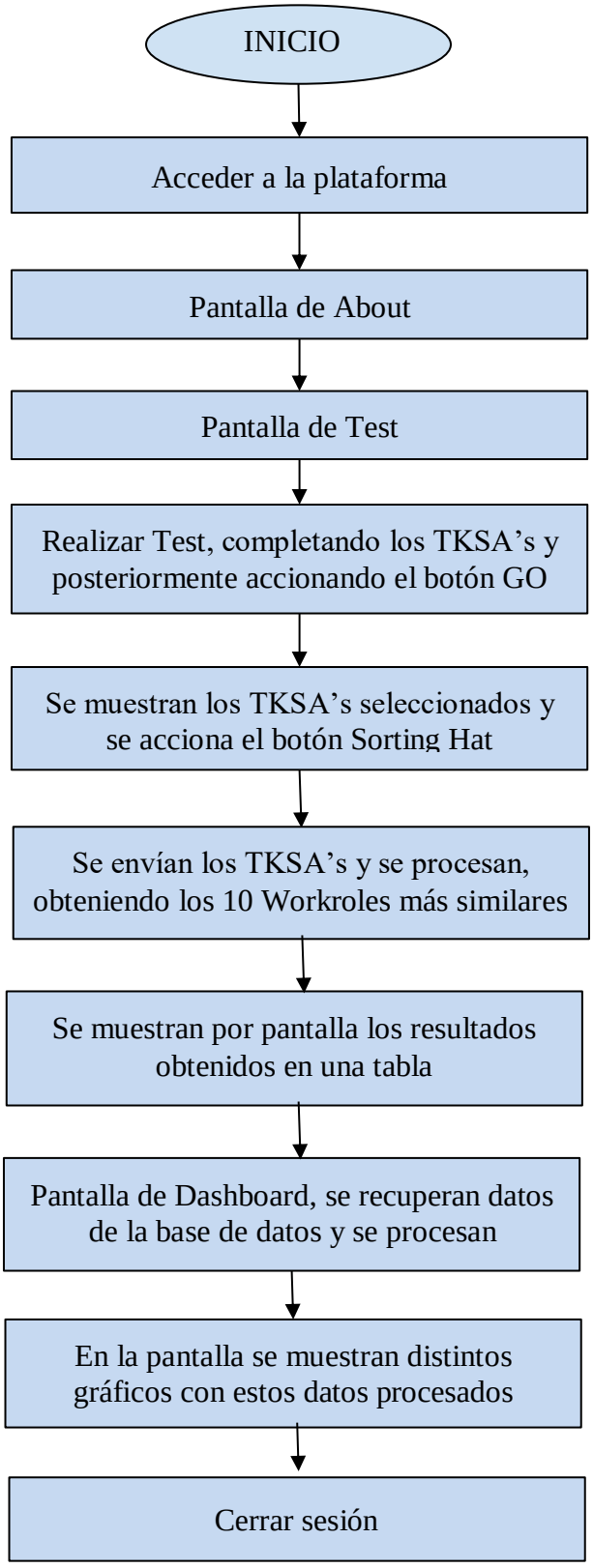


Figura 4.2. Diagrama de flujo de la aplicación

Previamente a acceder a la plataforma será necesario registrar un usuario. Para registrar un usuario, se introducen los valores en el formulario y una vez que se hace clic en el botón Registrar, se comprobará que el email no exista previamente en la base de datos. Por lo tanto, para registrar correctamente a un usuario la aplicación seguirá el siguiente diagrama de flujo.

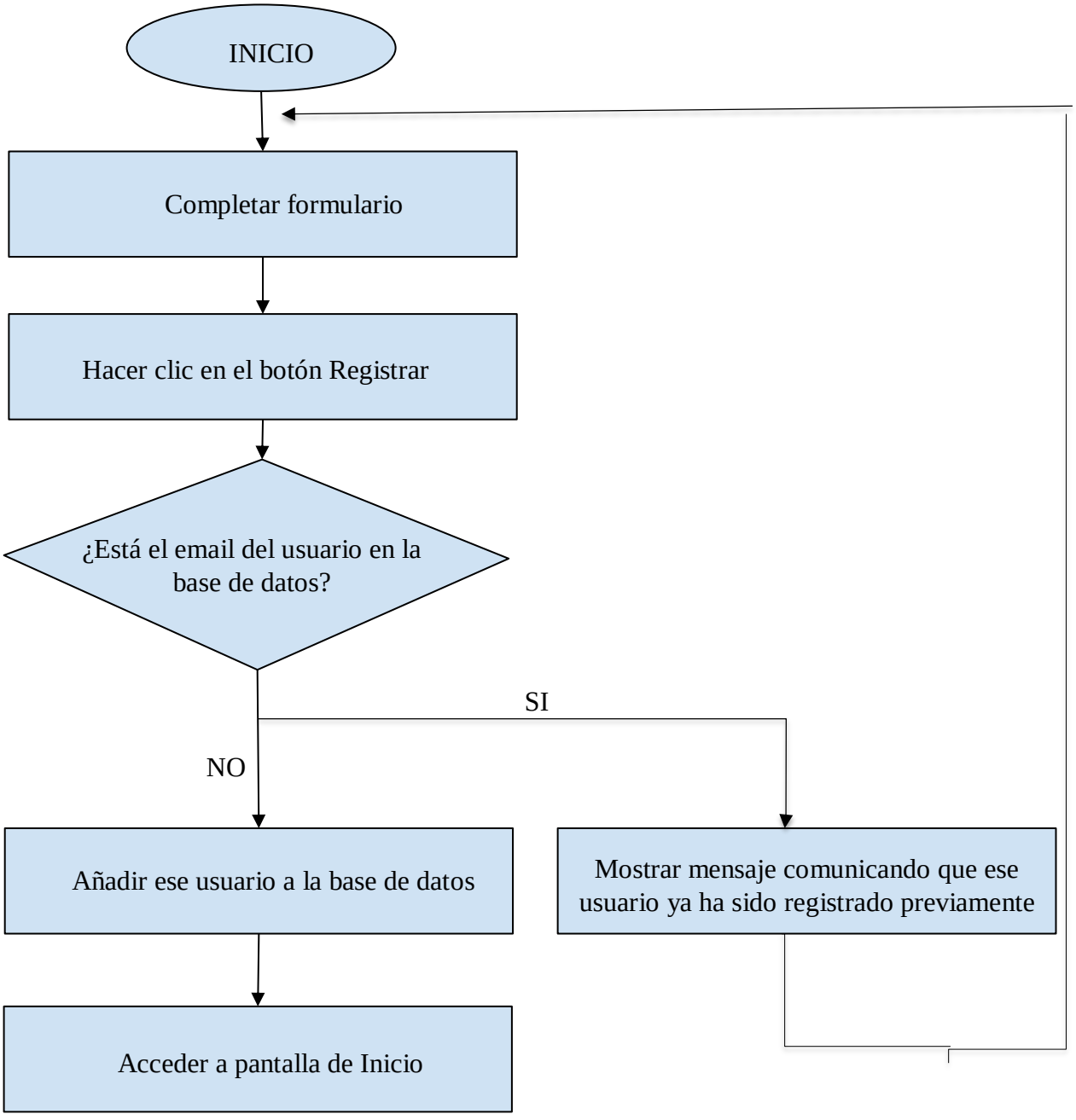


Figura 4.3. Diagrama de flujo de la registrar usuario

Realizar el test también es una tarea que, como se ha mencionado en apartados previos, debe acceder a la base de datos. Técnicamente se podría haber desarrollado de dos

formas, si el usuario ha tomado el test previamente podríamos preguntar si desea sobrescribir esos datos o directamente sobrescribirlos sin consultar al usuario asumiendo que si decide tomar el test de nuevo es debido a que ha cambiado su situación frente a la situación previa. Hemos decidido no preguntar al usuario si desea sobrescribir estos datos, por lo que el diagrama de flujo resultante sería el siguiente.

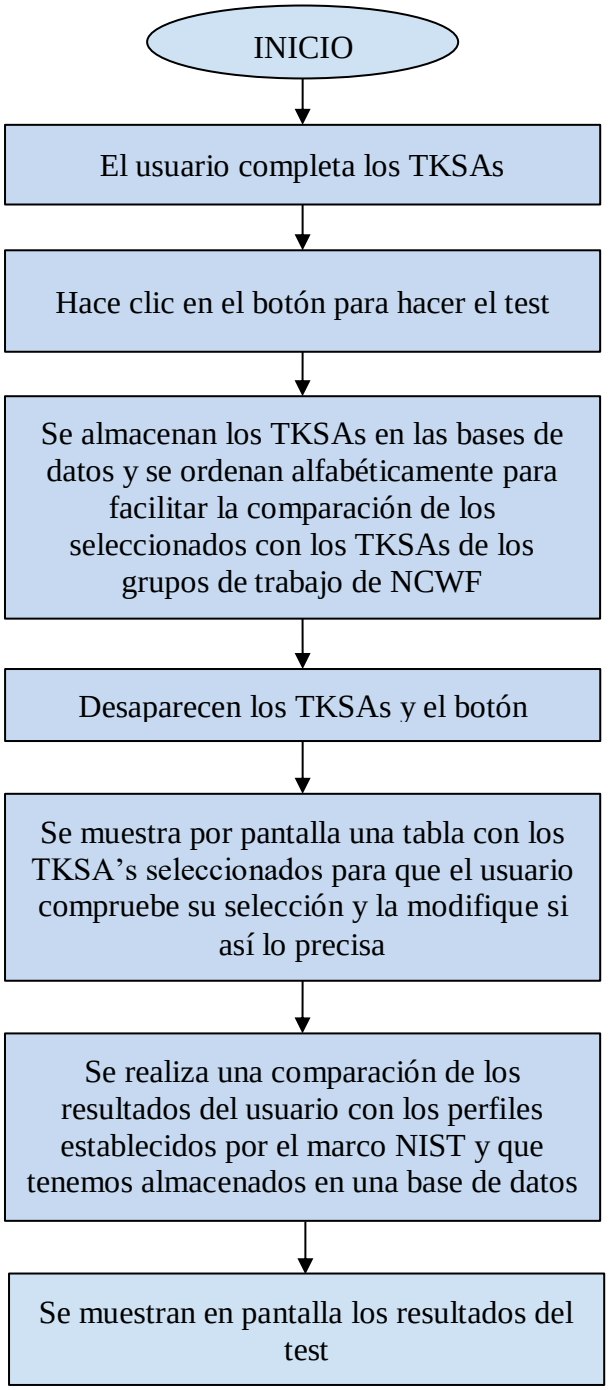


Figura 4.4. Diagrama de flujo de realizar test

4.3. Modificaciones del modelo previo.

Como ha sido mencionado previamente han sido necesarias una serie de modificaciones del proyecto anterior para optimizar y mejorar el proyecto final.

4.3.1. Base de datos

Las tablas de la base de datos forman parte del trabajo realizado por Javier Vila y por este motivo, no han sido explicadas en más profundidad para este proyecto.

A pesar de que no forman parte de este Trabajo Fin de Grado a continuación, podemos ver un esquema con las distintas tablas de la base de datos para facilitar la comprensión de la aplicación al lector.

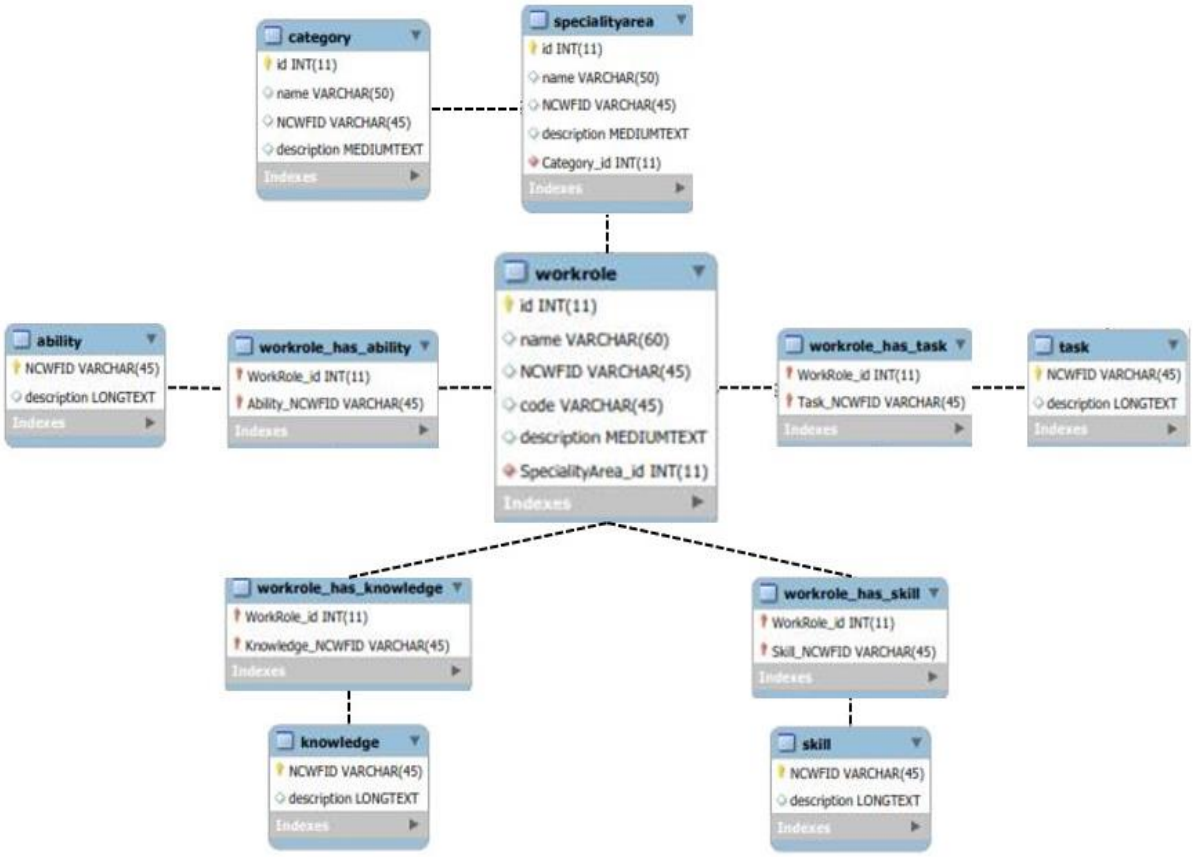


Figura 4.5. Base de datos

Con la finalidad de poder introducir usuarios y perfiles a la aplicación, se han añadido cuatro tablas de usuarios a la base de datos. Estas tablas, como se ha mencionado previamente, son competencia del TFG con nombre análogo a este. El contenido de estas tablas se muestra a continuación.

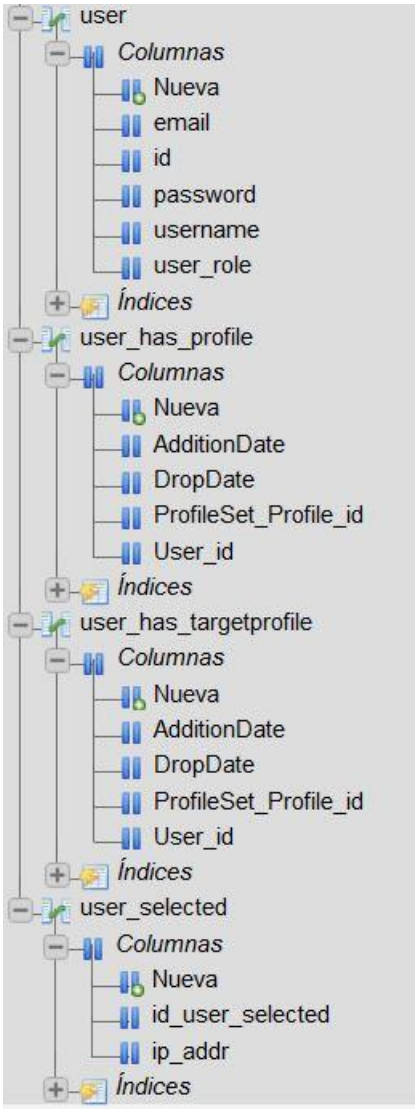


Figura 4.6. Tablas de la base de datos de usuario

4.3.2. Desarrollo del código de la aplicación

El desarrollador que realizó la primera versión del proyecto realizó un diseño de la aplicación que consistía en implementar toda la aplicación web en una única pantalla y mostrar u ocultar los elementos dependiendo del estado del proceso en el que nos encontráramos. Es decir, si el usuario estaba realizando la selección de TKSAs, la aplicación web hacía visible únicamente los elementos relacionados con este paso y mantenía ocultos el resto de elementos. En el diseño de este proyecto hemos decidido mejorar esta estructura y hemos creado realmente distintas páginas que coinciden con los distintos pasos que va a realizar un usuario. Hemos eliminado todo aquel código relativo a estos procesos y hemos rediseñado y recodificado la aplicación.

La finalidad de este cambio es proporcionar un desarrollo más claro e intuitivo. Cabe añadir que modificando la estructura previa facilitamos el aumento de funcionalidades del sistema. El desarrollo de futuras funcionalidades únicamente se verá influido por el desarrollo en sí y no por la preocupación de ocultar elementos de funcionalidades antiguas.

4.4. Entorno de desarrollo

Para poder desarrollar la aplicación web, los programadores hemos instalado en nuestros ordenadores Windows el programa XAMPP. XAMPP de Apache es el entorno más popular gratuito de desarrollo con PHP. Se trata de un servidor, para desarrollar aplicaciones en PHP, con conexión a base de datos SQL (LAMPP= Linux + Apache + MySQL + PHP + Perl). Se puede instalar en máquinas Windows, Mac OS X y Linux, pero la instalación varía de un sistema operativo a otro [20].

Para el desarrollo del código se ha utilizado el editor de texto Sublime Text.

4.5. Interfaz gráfica

Se ha rediseñado la interfaz gráfica de la aplicación y se ha programado desde cero para poder conseguir una interfaz clara, sencilla y atractiva para el usuario. Para que la aplicación sea visualmente más atractiva para el usuario se ha empleado Bootstrap. Bootstrap es un kit de herramientas de código abierto para desarrollar con HTML, CSS y JS. Contiene la biblioteca de componentes front-end más popular del mundo [21].

Al desarrollarse el proyecto bajo una metodología ágil, se han realizado varios diseños de la interfaz gráfica.

Se partió de un diseño inicial con una gama de colores llamativos para atraer la atención del usuario y con una estructura basada en cuadrantes. Tras varias modificaciones, se ha optado por un diseño en tonos blancos, grisáceos y negros con tonos pastel que contrastan para resaltar los elementos más importantes.

4.5.1. Estructura de la interfaz gráfica.

La aplicación consta de cuatro pantallas.

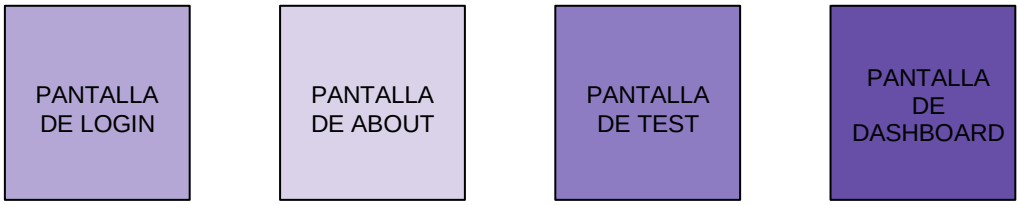


Figura 4.7. Esquema de pantallas presentes en la aplicación web del proyecto

La primera pantalla es la pantalla de Login, es la página en la que los usuarios podrán acceder al sistema o registrarse.

La segunda pantalla es la pantalla de About, se trata de la página de presentación del servicio. En esta sección podremos encontrar una barra de navegación que nos redirigirá a las dos pantallas siguientes. Observaremos un carrusel con imágenes y frases relativas a la seguridad de la información. Podremos encontrar adicionalmente una descripción del perfil de usuario. Finalmente encontraremos una descripción del servicio e información relativa al Framework de NICE que se utiliza para la categorización de perfiles.

La tercera pantalla es la pantalla de Test, en esta pantalla el usuario introducirá los TKSA's que posea para posteriormente presionar el botón de realizar test. Esta pantalla se divide a su vez en tres subpantallas. La primera subpantalla muestra los TKSAs que se encuentran en la base de datos, el usuario podrá seleccionar aquellos que posea y hará clic en un botón para acceder al siguiente paso. La segunda subpantalla mostrará los TKSAs que han sido seleccionados para que el usuario los modifique si así lo considera, en caso de no realizar modificaciones se pasará a la última subpantalla. Se realizará la comparación y análisis de las similitudes con los perfiles. Esta tercera subpantalla mostrará los resultados de la evaluación y asignará al usuario los diez perfiles y las diez categorías que más encajan con sus habilidades y conocimientos.

La cuarta y última pantalla es la pantalla de Dashboard, esta pantalla muestra gráficos relativos al usuario. Facilita así la visualización de los puntos fuertes y puntos a reforzar.

Se explicarán estas pantallas en más detalle en los siguientes apartados.

4.5.2. Pantalla de Login

Esta pantalla ha sido una novedad de este proyecto ya que la versión anterior no contaba con usuarios, y, por lo tanto, no era necesario autenticarse para acceder a los datos privados de estos. Se trata de una pantalla sencilla para que los usuarios puedan introducir sus credenciales y acceder al resto de funcionalidades.

En la versión Beta esta página se componía de dos formularios, uno para aquellos usuarios que tengan una cuenta y otro formulario para los que tengan que registrarse porque sean nuevos en la aplicación.

En cuanto al fondo del HTML podíamos encontrar un fondo de color negro, que en la segunda versión de la pantalla ha sido sustituida por una imagen relativa a la ciberseguridad. Este cambio se debe a que la desarrolladora ha tomado formación online sobre diseño de aplicaciones web, para poder desarrollar una página atractiva para el usuario, y esta formación enuncia que un diseño sencillo, pero con dimensiones es un diseño más atractivo para el usuario.

Adicionalmente, el formulario de registro contiene dos “radio buttons”, de los cuales solo se puede seleccionar uno. Estos selectores hacen referencia a los dos tipos de perfiles que podremos encontrar en la aplicación, uno para estudiantes y otro para empresas, este último se desarrollará en TFGs futuros y permitirá a las empresas acceder a funcionalidades extra que no tendrán los estudiantes, como publicar vacantes de ciberseguridad.

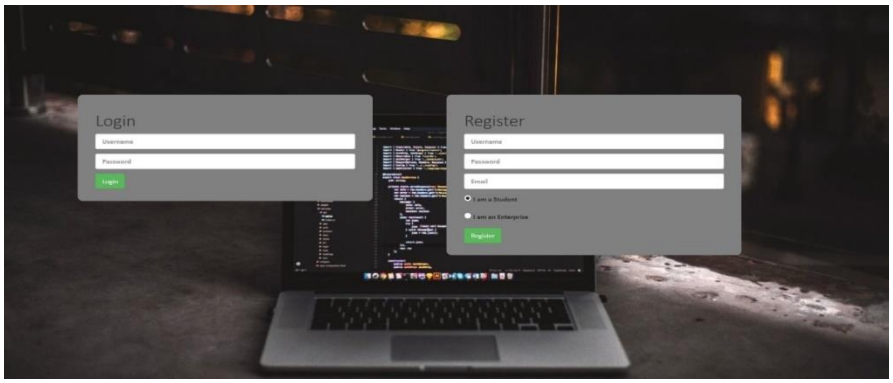


Figura 4.8. Captura de pantalla de la pantalla de login

4.5.3. Pantalla de About

La pantalla que aparece una vez nos hemos autenticado es pantalla de About.

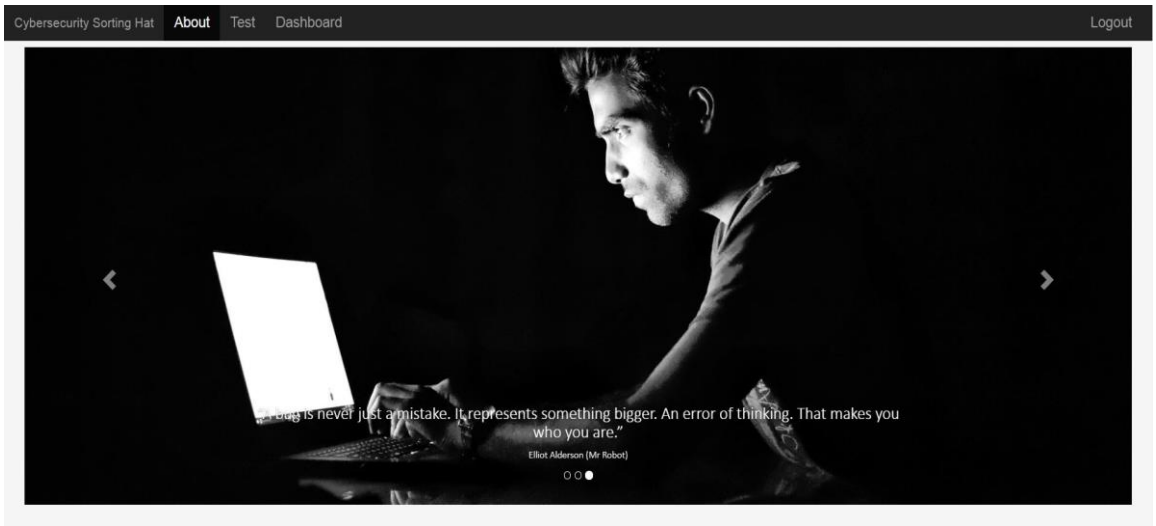
Esta página sirve de enlace entre la página de Login y la de acceso al Test. La versión anterior del proyecto carecía de esta pantalla que ha sido introducida para proporcionar mayor nivel de formalidad y seriedad a la aplicación.

Se ha añadido una barra de navegación en color carbón desde la cual el usuario puede acceder al resto de páginas. En esta barra el usuario podrá cerrar sesión cuando termine de usar la aplicación.

En esta sección podremos encontrar una barra de navegación que nos redirija a las dos pantallas siguientes. Observaremos un carrusel con imágenes y frases relativas a la seguridad de la información. Podremos encontrar adicionalmente una descripción del perfil de usuario. Finalmente encontraremos una descripción del servicio e información relativa al Framework de NICE que se utiliza para la categorización de perfiles.

Para obtener la información de perfil relativa al usuario se hacen consultas a la base de datos para que devuelva la información.

A continuación, podemos ver cómo sería la pantalla para un usuario estudiante, equivale a un usuario "common" (común), de nombre Sandra y con email Sandra@gmail.com.



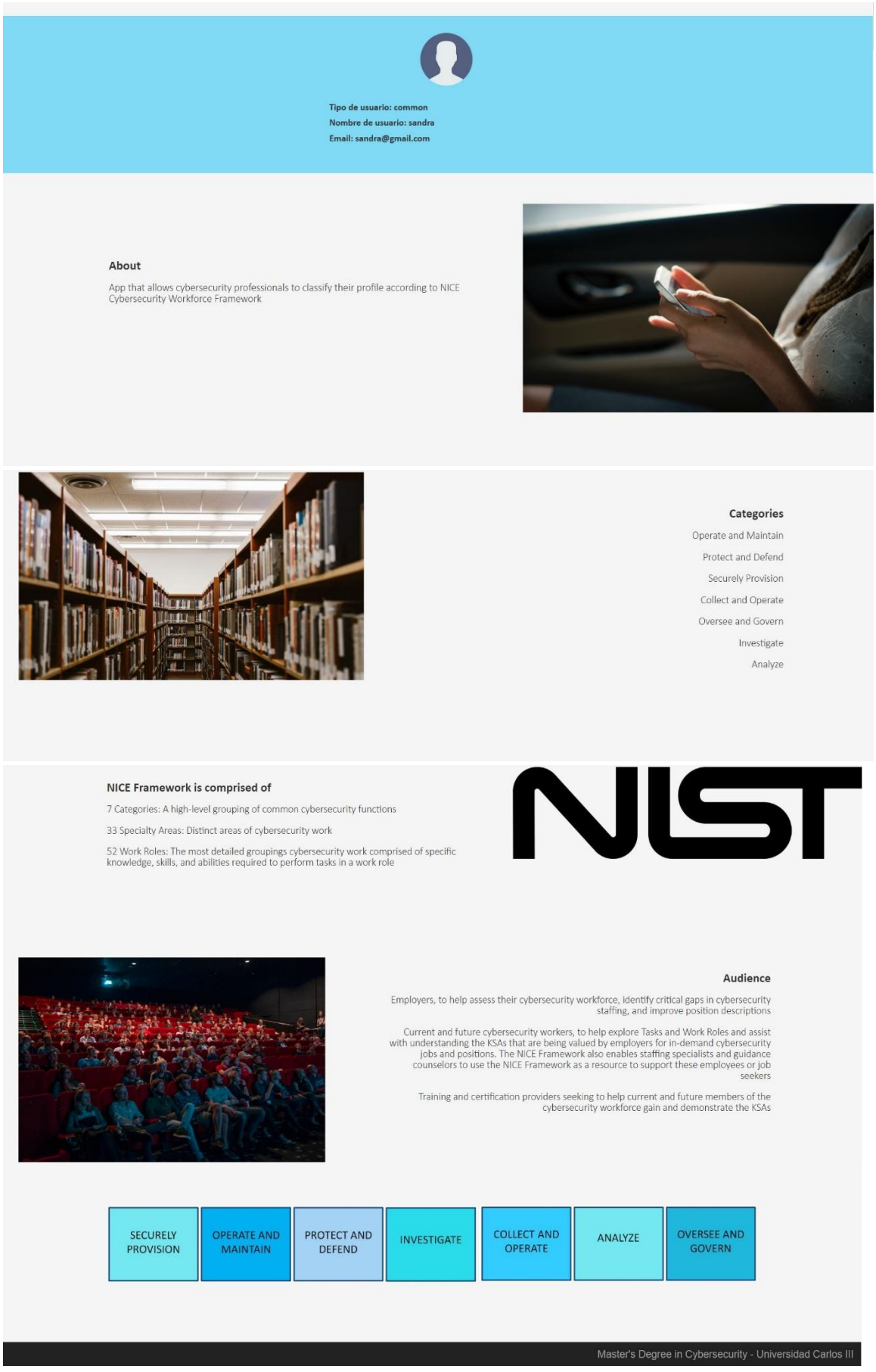


Figura 4.9. Captura de pantalla de la pantalla de Inicio

4.5.4. Pantalla de Test

Esta pantalla se muestra una vez que hemos hecho clic en la pestaña Test. Se trata del núcleo de la aplicación web puesto que en esta vista el usuario seleccionará los TKSAs que posee y se mostrará el perfil al que corresponde.

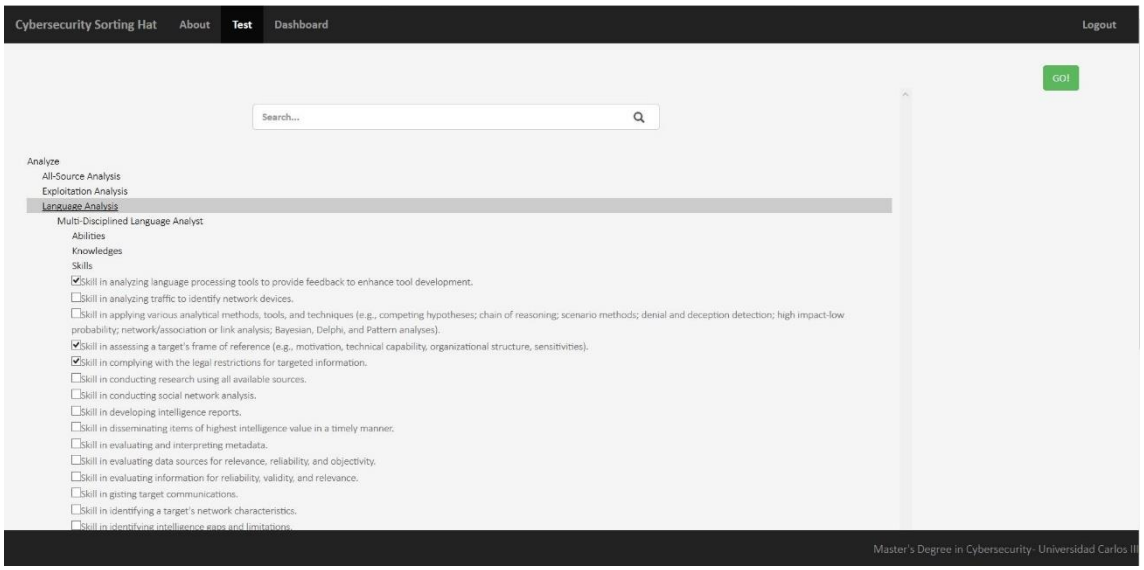


Figura 4.10. Captura de pantalla de la pestaña de Test

Como podemos observar en la figura 4.18, la vista se divide en dos columnas, la primera columna incluye los TKSAs con "checkbox" para que el usuario los seleccione. En la segunda columna podremos encontrar el botón que seleccionará el usuario una vez que haya rellenado los TKSAs.

En cuanto a la lógica del sistema, estos TKSAs se muestran en un árbol dinámico, se trata de la opción más óptima puesto que permite a los usuarios expandir y reducir los nodos, y de esta manera, facilita al usuario a encontrar los TKSAs que posee y a completar el test.

Una vez que el usuario haya accionado el botón de "GO" se almacenarán estos TKSAs por orden alfabético y se guardarán en un Array que se mandará a back-end para almacenarlo en la base de datos. Este Array tiene a forma:

Array ["A056", "A068", "K0032", "T1221", "T0564"]

Donde cada uno de los argumentos del array es el ID que corresponde al TKSA seleccionado.

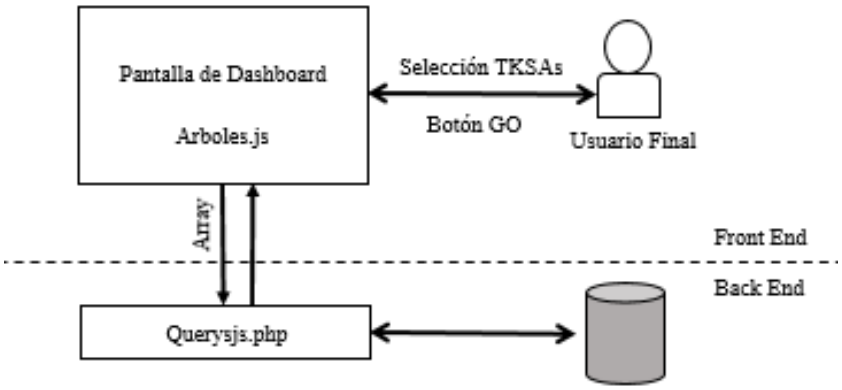


Figura 4.11. Esquema de las transiciones al pulsar el botón GO

Cuando los datos hayan sido enviados se construirá sobre esta pestaña una segunda vista que se compone de una tabla con los TKSAs que el usuario había seleccionado, por si desea modificar su selección.

Para la construcción de esta pantalla es necesario un array que contiene el identificador de los TKSAs, el nombre de los TKSAs y la descripción de estas. Este array se construye en el Javascript, realizando las consultas correspondientes y posteriormente se construye una tabla sobre la que se imprime este array.

Adicionalmente en esta vista se sustituye el botón anterior de “GO” por tres botones. “Sorting Hat” conduce al usuario a la pantalla final del test. “Go Back” permite al usuario volver a la pantalla anterior, mostrándole su selección para que pueda editarla. “Start over” vacía la cache y comienza el proceso desde el principio, el usuario tendrá que completar los TKSAs desde cero. Cada uno de estos botones cuenta con funciones distintas de Javascript.

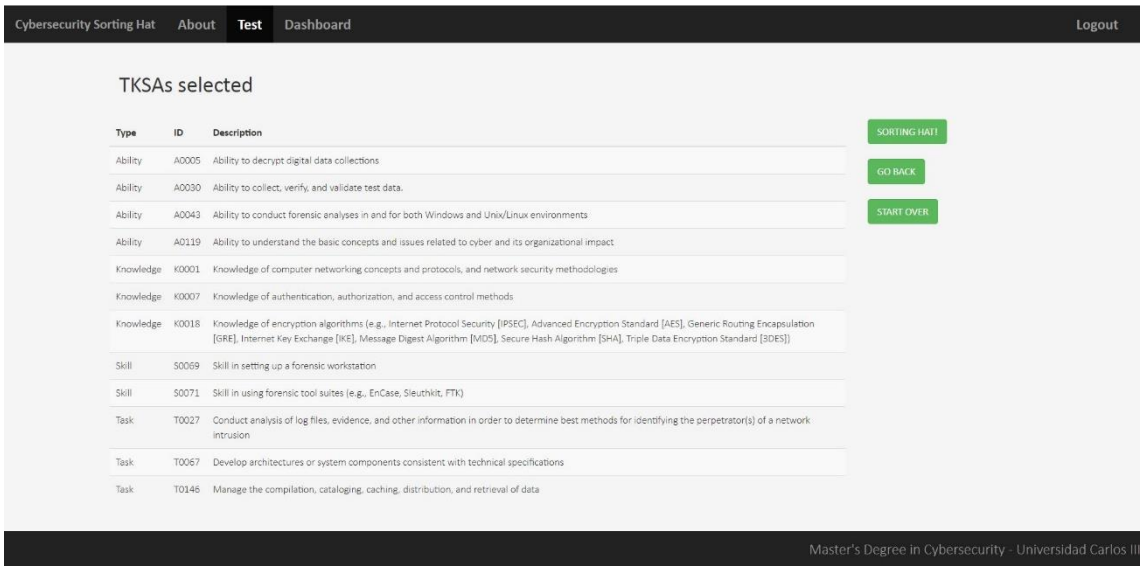


Figura 4.12. Captura de pantalla de Test después de accionar el botón GO

Cuando el usuario presiona el botón "Sorting Hat" se mostrarán los diez workroles y las diez categorías con los que el usuario tiene un mayor grado de similitud, calculado en porcentajes.

Esta información se encuentra organizada en seis arrays:

- Array 0: contiene resultados de "abilities"
- Array 1: contiene resultados de "knowledges"
- Array 2: contiene resultados de "skills"
- Array 3: contiene resultados de "tasks"
- Array 4: contiene resultados de todos los TKSAs.
- Array 5: contiene los nombres de los workroles.

La construcción de estos resultados es un procedimiento que debe hacerse en back-end, ya que las operaciones necesitan realizarse directamente sobre la base de datos. Puesto que forma parte de uno de los proyectos realizado por uno de los compañeros, no entraremos en más detalle sobre ese procedimiento.

El cálculo de estas similitudes consiste en un bucle que recorre todos los workroles y categorías disponibles en la base de datos. Posteriormente, se calcula el porcentaje comparando el perfil del usuario que ha tomado el test con los TKSAs de cada uno de los workroles de la base de datos.

Los resultados se muestran de manera ordenada, de mayor porcentaje de coincidencia a menor.

La pantalla consta de dos botones, cuando accionamos el botón de "TOP 10 Workroles" se muestran los diez workroles con mayor grado de compatibilidad con el usuario.

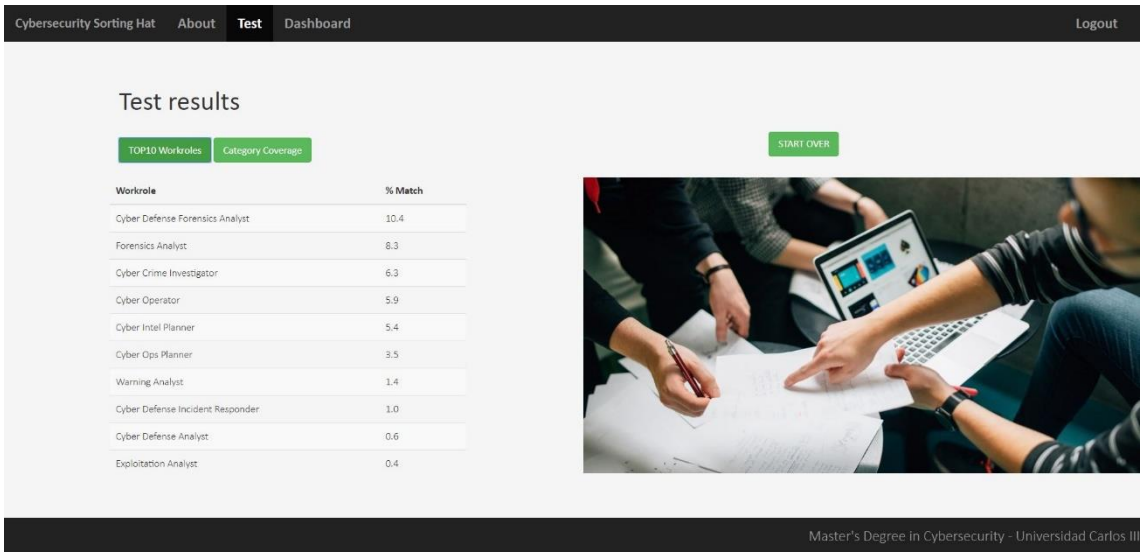


Figura 4.13. Captura de pantalla de Test: 10 Workroles

Cuando accionamos el botón de Category Coverage se muestran las siete categorías del NCWF Framework ordenadas de mayor a menor coincidencia con el perfil de usuario.

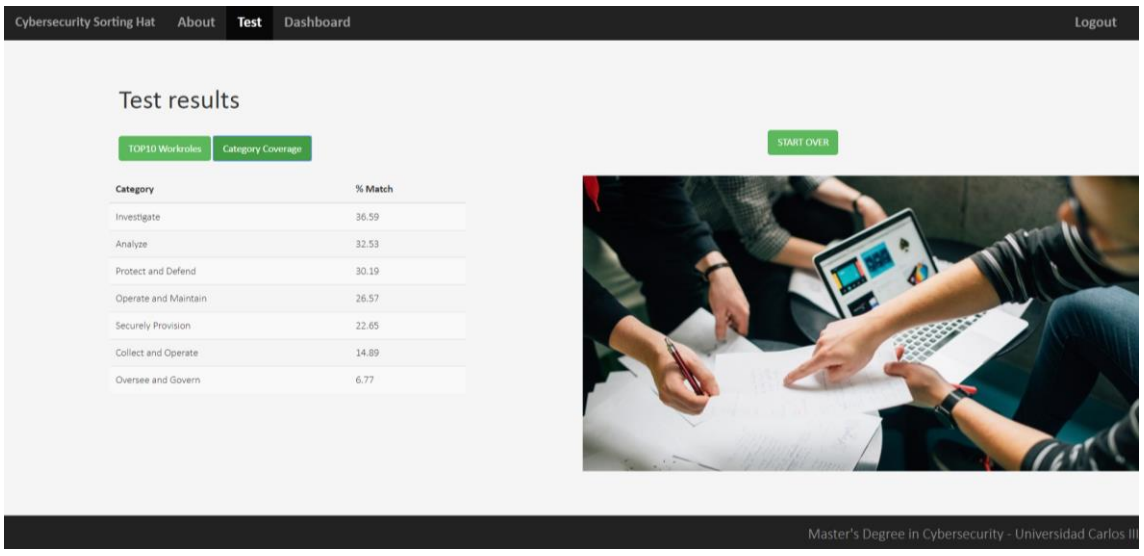
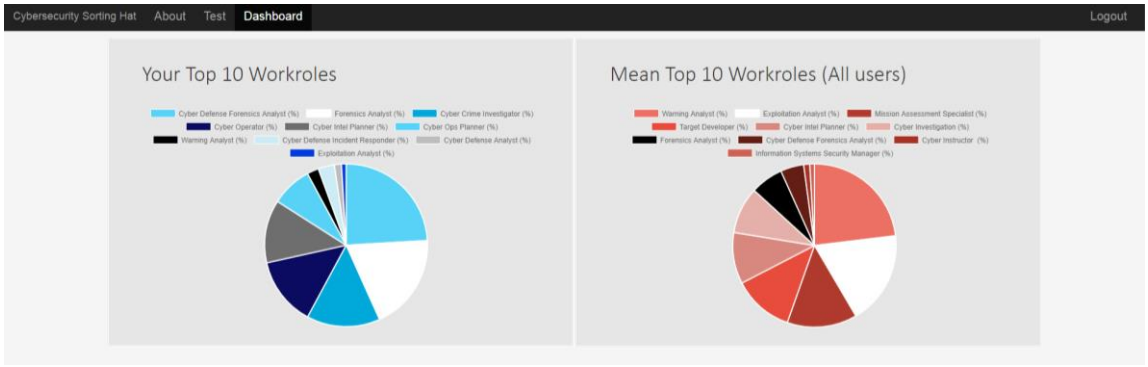


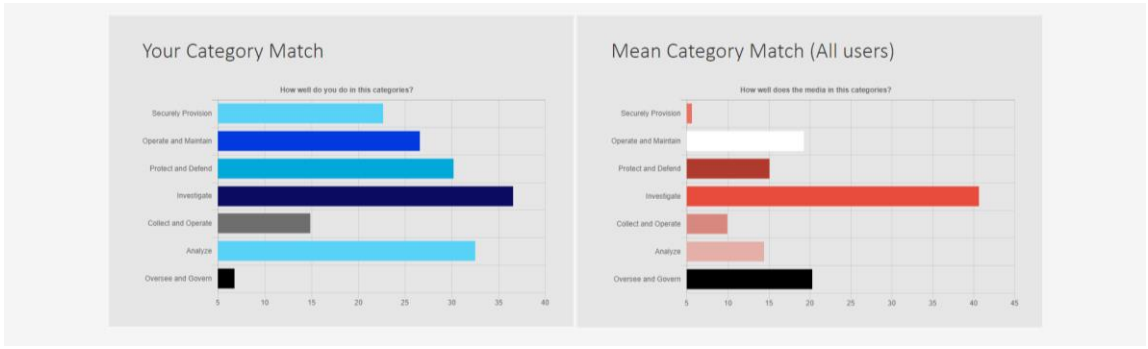
Figura 4.14. Captura de pantalla de Test: 10 categorías

4.5.5. Pantalla de Dashboard

La pantalla de Dashboard ha sido la más costosa de desarrollar, puesto que la realización de gráficos con estadísticas procesando datos recogidos de la base de datos no se había visto en ninguna asignatura y ha sido necesario formarse adicionalmente para poder realizar este requisito.

Podemos dividir la pantalla de Dashboard en dos tipos diferentes de gráficos, en azul se muestran aquellos relativos al usuario que está autenticado y en rojo se muestran los que corresponden a la media de usuarios de la aplicación web.





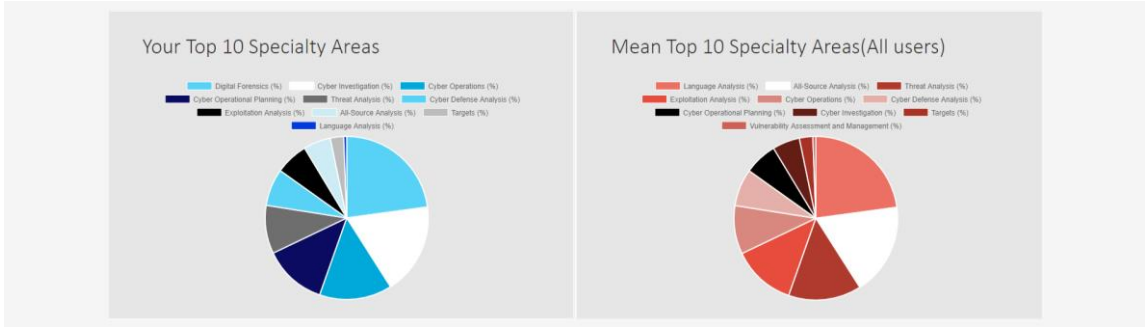


Figura 4.15. Captura de pantalla de la pestaña de Dashboard

Para poder utilizar Dashboard es necesario usar la siguiente lógica: cuando el usuario acciona el botón de realizar test, los datos se almacenan en la base de datos. Para poder realizar los dashboards se accederá a las bases de datos y se procesará esta información para poder representarla.

Se han barajado distintas librerías para apoyarse en la representación de gráficos. Entre ellas podíamos encontrar algunas públicas y gratuitas publicadas en la página Github, otras propuestas por Google como Google Chart y otras no Open Source como CanvasXpress. Finalmente, se ha optado por emplear la librería chart.js puesto que tenía un diseño sencillo pero llamativo y proporcionaba una mayor variedad de gráficas que su competencia.

Antes de entrar en detalle acerca de los mecanismos que se han usado para recuperar la información y representarla es importante recordar que el desarrollador que implementaba la capa de datos y gran parte de la capa de negocios no ha podido finalizar su parte antes de que este TFG se presente. Por lo tanto, los datos representados en las capturas de pantalla no son datos reales de un usuario, sino que se han realizado para poder exponer los requisitos cumplidos en este proyecto.

Se debe mencionar también que el código se ha preparado para que el otro desarrollador únicamente iguale las variables de los usuarios a las variables generales que se han utilizado para el desarrollo del código. A continuación, se muestra un ejemplo de este.

```
new Chart(document.getElementById("pie-chart"), {
    type: 'pie',
    data: {
      labels: [workrole1, workrole2, workrole3, workrole4, workrole5,workrole6, workrole7, workrole8, workrole9, workrole10],
      datasets: [{
        label: "% of similarities",
        backgroundColor: ["#58D3F7", "#FFFFFF","#01A9DB","#0B0B61","#6E6E6E","#58D3F7","#000000", "#CEECF5", "#BDBDBD", "#013ADF"],
        data: [porcentaje1,porcentaje2,porcentaje3,porcentaje4,porcentaje5,porcentaje6,porcentaje7,porcentaje8,porcentaje9,porcentaje10]
      }]
    },
});
```

Figura 4.16. Código preparado para el siguiente desarrollador

Primero explicaremos los gráficos que corresponden al usuario que se ha autenticado.

Los gráficos escogidos han sido:

- **De barras**: para representar el porcentaje de coincidencia con cada una de las 7 categorías establecidas por el NICE Framework.

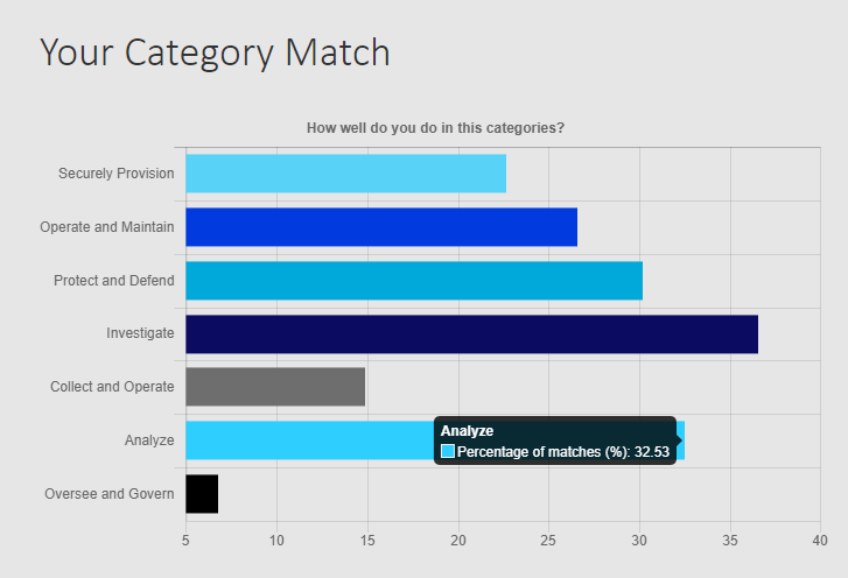


Figura 4.17. Ejemplo gráfico de barras

En lo referente al desarrollo, este gráfico accede a la base de datos donde se encuentran almacenados los TKSAs resultantes del test, es decir, todos aquellos que fueron seleccionados en la pantalla de los checkbox. Se realiza un bucle que suma los TKSAs que pertenecen a una misma categoría.

Posteriormente, se calcula el porcentaje de coincidencias comparando el número de TKSAs que tiene el usuario frente a TKSAs totales para cada categoría. Este valor se muestra en “Percentage of Matches (%)” de la pestaña emergente que aparece cuando sitúas el cursor sobre cada una de las barras del gráfico.

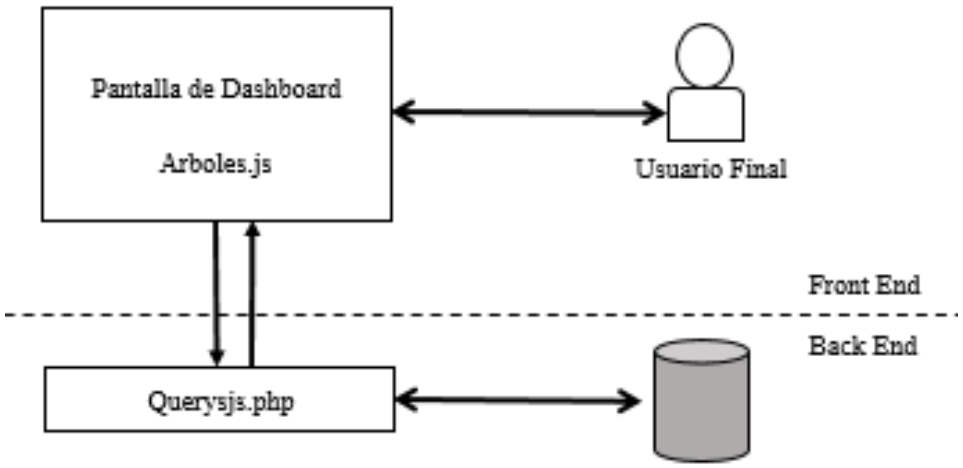


Figura 4.18. Esquema de las transiciones al acceder a la página de Dashboard

Como podemos ver en la figura anterior es necesario solicitar y recuperar la información que se devuelve en forma de arrays.

Puesto que como no están desarrollados los usuarios, se ha entregado el código al compañero con variables. Estas variables actualmente se encuentran inicializadas a un valor fijo que posteriormente se sustituirá por los arrays correspondientes del usuario como se ha comentado anteriormente.

- **De tarta:** Hemos seleccionado este gráfico para representar el TOP 10 de Workroles que se había mostrado previamente al realizar el test.

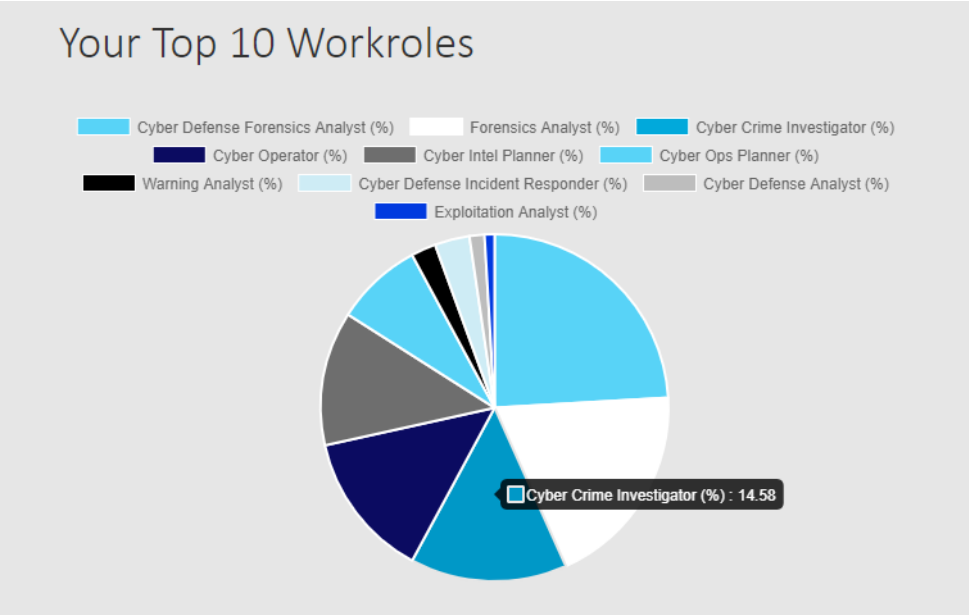


Figura 4.19. Ejemplo gráfico de tarta Workroles

En lo referente al desarrollo, este gráfico accede a la base de datos donde se encuentran almacenados los resultados del test, concretamente al array que posee los workroles y el porcentaje de similitud con cada uno de los grupos de trabajos definidos por el NCWF.

Este gráfico equivale a la tabla que se ha mostrado al final de tomar el test. En la pestaña emergente se muestra el nombre del grupo de trabajo y el porcentaje de similitud que le corresponde. Puesto que la suma de estos diez porcentajes no tiene por qué ser un 100%, se realiza una proporción para ordenar los diez perfiles profesionales más similares y que sumen un 100%.

Para obtener estos resultados tenemos que recuperar los arrays calculados para la pestaña de Test y representarlos.

Para obtener el segundo gráfico de tarta "Top 10 Specialty Areas" se procesa el Array de los workroles con el mayor número de similitud y se obtienen sus áreas de especialidad. En el caso de estas áreas se pueden repetir para distintos workroles, por lo que se procesará el array de workroles desde el principio y se irán rellenando las variables de áreas de especialidad con áreas distintas. Es decir, si los tres primeros workroles comparten área de especialidad, se asignará esa como la primera área y se continuará recorriendo el array hasta que encontremos diez áreas de especialidad diferentes.

Al igual que para el gráfico anterior, se mostrará en una pestaña emergente el porcentaje de similitud. Este porcentaje se ha calculado sobre un 100% realizando las mismas proporciones que para el gráfico anterior.

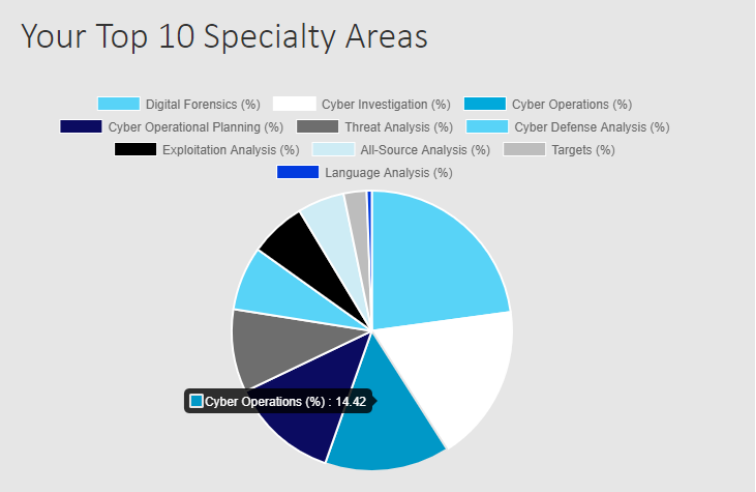


Figura 4.20. Ejemplo gráfico de tarta Specialty Areas

- **De donut:** para mostrar el porcentaje de usuarios que son estudiantes frente al porcentaje de usuarios que pertenecen a una empresa. Puesto que el desarrollo de perfil de empresa se realizará en futuros trabajos, actualmente el gráfico cuenta con un 100% de usuarios con perfil de estudiante.

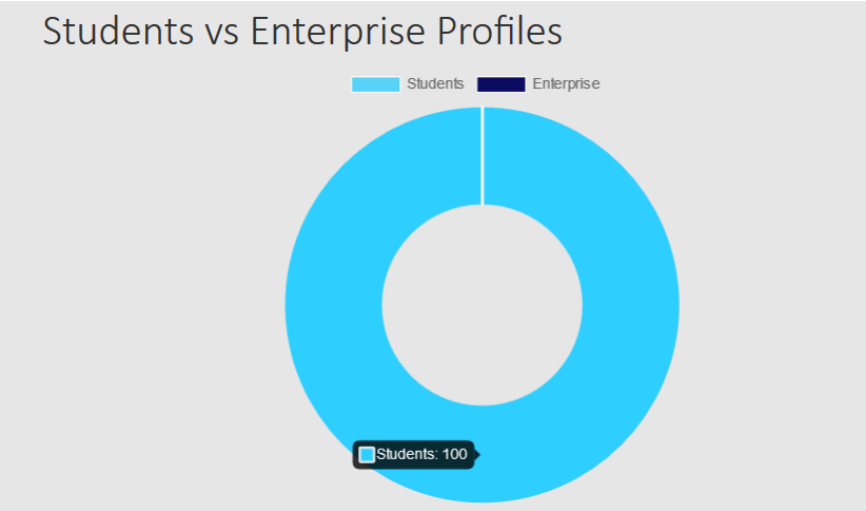


Figura 4.21. Ejemplo gráfico de donut

Como mencionamos en el apartado de pantalla de login, el perfil de empresa se desarrollará en proyectos posteriores por lo que en la actualidad el 100% de los usuarios serán usuarios de tipo estudiante.

En lo referente al desarrollo, este gráfico accede a la base de datos donde se encuentran almacenados los usuarios. Comprueba el tipo de todos los usuarios que estén registrados y realiza una suma de cada tipo. Es decir, por una parte, tendremos un X de perfiles estudiantes y por otra un Y de perfiles de empresa. Finalmente representaremos en la gráfica X frente a Y.

A continuación, se muestran los gráficos que corresponden a la media de usuarios de la aplicación.

Para calcular esta media de usuarios se creará, en proyectos posteriores, un usuario al que se le almacenará la información relativa al resto. Es decir, un usuario estudiante posee únicamente su información, los TKSAs que ha seleccionado y los resultados de su test, sin embargo, el usuario "media" almacenará la media de los resultados de todos los usuarios que estén dados de alta y hayan realizado el test.

En cuanto al desarrollo, se añadirá en el proceso de obtención de resultados de test que esta información, el array que contenía todos los datos y que se ha explicado en apartados previos, se guarde en el usuario autenticado y en el usuario media.

Puesto que el desarrollo de esas nuevas funcionalidades no entra en el alcance de este proyecto, para este se han dejado las estructuras, en función de variables para que simplemente se tenga que sustituir el valor al que está actualmente inicializadas las variables por las variables que accedan al usuario "media".

Los gráficos escogidos han sido:

- **De barras**: para representar la cantidad de coincidencias con cada una de las 7 categorías establecidas por el NICE Framework. El funcionamiento de este gráfico es igual que para el usuario autenticado, pero se muestran los datos de usuario "media".

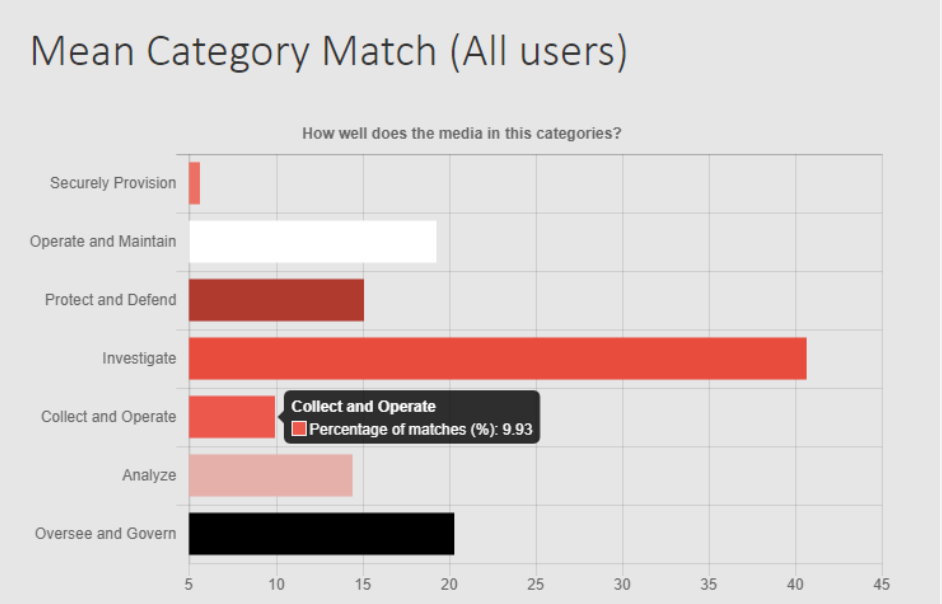


Figura 4.22. Ejemplo gráfico de barras usuario media

- **De tarta:** Hemos seleccionado este gráfico para representar el TOP 10 de Workroles que se había mostrado previamente al realizar el test. El funcionamiento de este gráfico es igual que para el usuario autenticado, pero se muestran los datos de usuario "media".

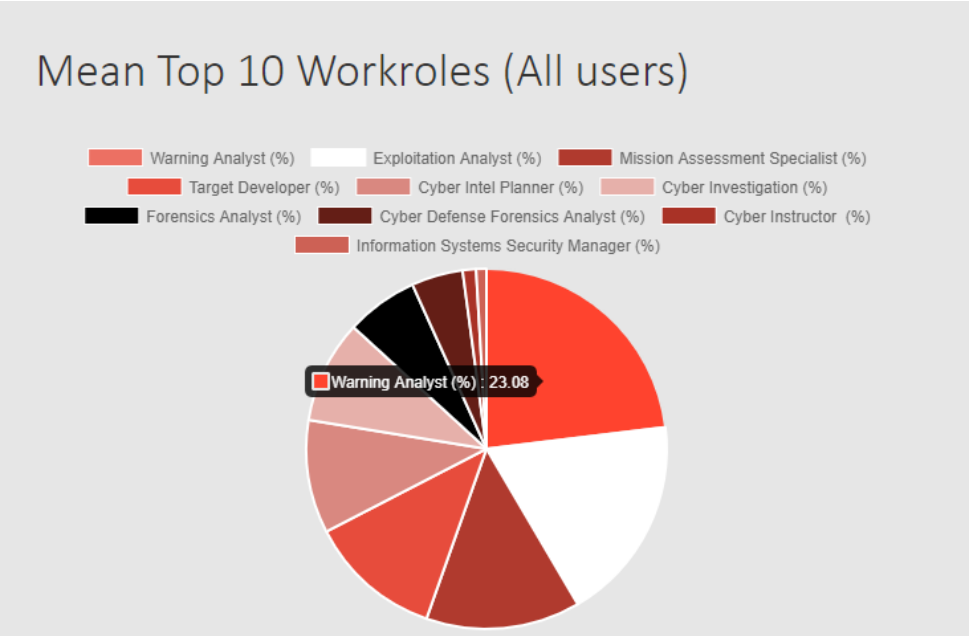


Figura 4.23. Ejemplo gráfico de tarta workroles usuario media

Al igual que en el caso anterior, en este gráfico se representan las diez áreas de especialidad con mayor grado de coincidencia para la media. Los datos se obtienen de la misma manera que para el usuario autenticado, pero obteniendo los datos del usuario media.

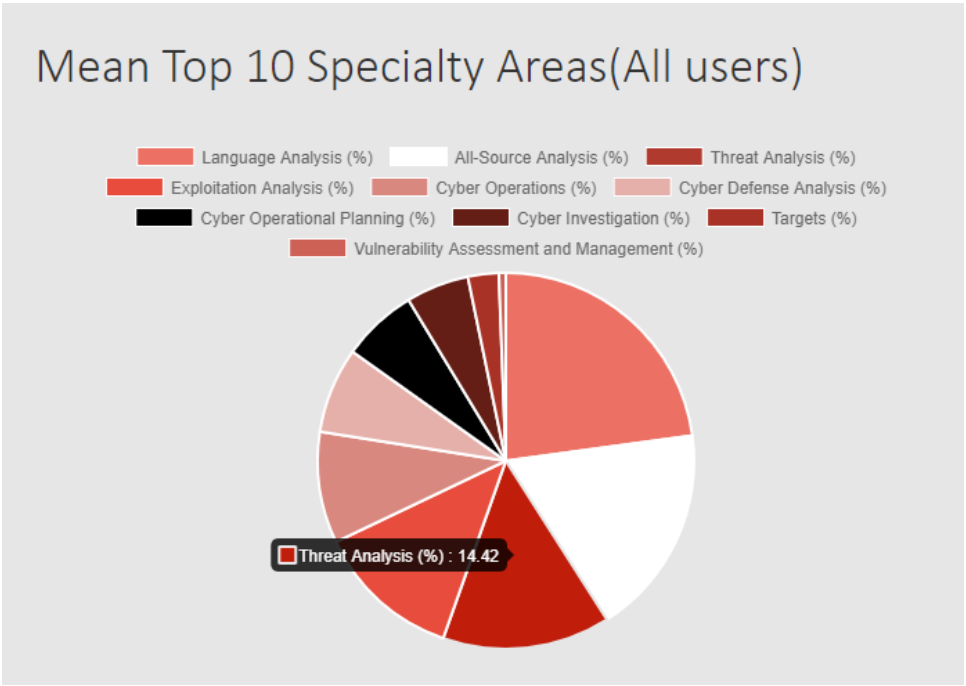


Figura 4.24. Ejemplo gráfico de tarta specialty areas usuario media

4.6. Pruebas UX

Para comprobar que se trata de una interfaz gráfica intuitiva se han realizado distintas pruebas de User Experience. Se ha realizado una entrevista a una muestra de 5 alumnos de la Universidad Carlos III.

Las entrevistas UX consisten en grabar pantalla y audio y pedir a los usuarios distintas tareas que estén relacionadas con la aplicación web para comprobar si consiguen realizar las acciones sin problemas o si por el contrario la interfaz no es intuitiva y es complejo terminar el proceso de búsqueda de perfil profesional.

Como se ha mencionado en varias ocasiones, falta el trabajo de otro compañero por lo que las pruebas de User Experience se han simulado completando pantallas semi estáticas y en el caso del Dashboard se ha pedido interpretar uno que se ha proporcionado ya representado, sin gráficos reales.

Para realizar estas pruebas se ha utilizado el programa Camtasia Studio 9 que cuenta con un grabador de pantalla y de micrófono denominado Camtasia Recorder.

Las tareas asignadas a los usuarios han sido:

- Registrarse como usuarios.
- Acceder a la plataforma y realizar el test para determinar a qué perfil pertenecen. Debemos tener en cuenta que los usuarios entrevistados no eran profesionales de la seguridad de la información, por lo tanto, han seleccionado TKSA's aleatorios.
- Consultar el apartado de Dashboard para comprobar si realmente es sencillo ver las debilidades y fortalezas del usuario.

Las tablas con los cuestionarios que se han realizado se encuentran en el Anexo B.

Las conclusiones que se han obtenido de estos cuestionarios son las siguientes:

- Un 75% de los entrevistados tienen un perfil técnico, frente a un 25% que han estudiado una carrera de la rama de ciencias sociales.
- Un 100% de los entrevistados sabe a qué institución corresponde la aplicación web.

- Un 25% relaciona los colores con los de la institución, el 75% restante no relaciona los colores, pero afirma que hay elementos como el logo en la pestaña del navegador que relaciona con los colores.
- Un 100% de los entrevistados conoce la audiencia a la que está dirigida la aplicación web, lo comprobaron en la pestaña About y en la barra de navegación inferior.
- Un 100% de los entrevistados remarca su satisfacción con la selección de contenidos destacados en la portada.
- Un 100% de los entrevistados ha conseguido completar exitosamente el proceso para realizar el test.
- Un 100% de los entrevistados ha conseguido registrarse como usuario sin tener ninguna duda. Para esta pregunta cabe destacar que primero se explicó a los entrevistados que tenían que simular ser estudiantes.
- Un 75% de los entrevistados ha entendido el Dashboard y un 25% ha necesitado alguna explicación adicional de los resultados.

4.7. Seguridad

Como hemos mencionado al comienzo de este documento, la seguridad en la actualidad es vital. Es necesario proteger nuestras aplicaciones de los posibles ataques que puedan producirse.

Con la finalidad de proteger la información de nuestra aplicación se ha revisado el TOP 10 de vulnerabilidades de OWASP [22] y se han tomado una serie de medidas que se detallan a continuación.

OWASP es una organización mundial sin ánimo de lucro enfocada en mejorar la seguridad del software. [23]

Figura 4.25. Top 10 de vulnerabilidades OWASP

4.7.1. Inyección

Esta vulnerabilidad conocida como Inyección SQL consiste en que el atacante aprovecha una debilidad o falta de seguridad en las querys que acceden a la base de datos.

Por ejemplo, en la autenticación del usuario, si el formulario no está correctamente protegido, el atacante podría acceder a un usuario que no fuera el suyo sin introducir la contraseña.

La solución a esta vulnerabilidad es separar los datos sensibles del usuario de la consulta que se haga a la base de datos. En el caso del código de esta aplicación podemos ver protección frente a inyección en procesos como la autenticación del usuario o el registro de este.

4.7.2. Autenticación rota y gestión de sesiones

Las funciones de aplicación relacionadas con la autenticación y la administración de sesiones a menudo no se implementan correctamente, lo que permite a los atacantes

comprometer contraseñas, claves o tokens de sesión, o explotar otros defectos de implementación para asumir las identidades de otros usuarios. [22]

La base de datos ha sido protegida con usuario y contraseña que sólo conocen los desarrolladores de este proyecto, de esta manera, impedimos que cualquier usuario de la aplicación pueda acceder a la base de datos y manipularla.

Uno de los principales ataques en esta vulnerabilidad se realiza cuando se solicita un recordatorio de contraseña y este proceso no está suficientemente verificado. Puesto que esta opción no está implementada no contamos con este tipo de vulnerabilidad.

4.7.3. Conexión PHP, Vulnerabilidad de control de acceso

Para proteger la aplicación se han extraído del PHP los parámetros que se utilizan para la conexión y se han movido a otro documento en otra carpeta.

```
require "../connect.inc.php";
$enlace = new mysqli($Host, $User, $Password, $DBName);
```

5. PLANIFICACIÓN Y PRESUPUESTO

5.1. Planificación temporal del proyecto

El desarrollo del proyecto ha tenido una duración de cuatro meses. Ha seguido una planificación propuesta al inicio de este ya que era necesaria la coordinación de dos desarrolladores.

Para realizar esta planificación se ha desarrollado un diagrama de Gantt con las funciones que se han desempeñado en este proyecto y la duración de estas.

En rosa están especificadas las funciones que han sido realizadas por la desarrolladora de este proyecto y en verde por el cliente del proyecto, en este caso, la tutora del Trabajo Fin de Grado.

TABLA 5.1. DIAGRAMA DE GANTT CON LA PLANIFICACIÓN DEL PROYECTO

Tareas/Fechas	1ª quincena de Febrero	2ª quincena de Febrero	1ª quincena de Marzo	2ª quincena de Marzo	1ª quincena de Abril	2ª quincena de Abril	1ª quincena de Mayo	2ª quincena de Mayo	1ª quincena de Junio	2ª quincena de Junio	1ª quincena de Julio
Especificación de requisitos											
Lectura de documentación											
Formación Desarrollo Aplicaciones web											
Planificación del proyecto											
Estudio del proyecto anterior para rediseñarlo											
Diseño del proyecto (I)											
Desarrollo del código (I)											
Pruebas (I)											
Diseño del proyecto (II)											
Desarrollo del código (II)											
Pruebas (II)											
Realización de la memoria											
Corrección de la memoria											
Comprobación de detalles finales											
Entrega del proyecto											
Defensa del proyecto											

Tareas realizadas por: Sandra Sánchez Esperante; Ana Isabel González-Tablas Ferreres

5.2. Presupuesto

El proyecto no ha necesitado una inversión CAPEX en infraestructura física o bienes materiales. Se trata de un proyecto software por lo que los costes provienen directamente del coste de las horas que han empleado los integrantes de este.

Para el desarrollo del proyecto se ha elegido a una programadora Junior, esto beneficia al cliente porque reduce los costes frente a tratarse de un programador Senior.

Se ha utilizado la calculadora de salario medio disponible en la aplicación web Guía Salarial [24], esta calculadora media ha sido proporcionada por los Servicios de Orientación y Empleo de la Universidad Carlos III.

Acorde con la estimaciones que proporciona la calculadora, un desarrollador PHP en Madrid con una experiencia entre 0-2 años tiene un sueldo medio de 25.000€/anuales lo que equivale a aproximadamente 11.16€/hora y un desarrollador de UX en Madrid con una experiencia entre 0-2 años tiene un sueldo medio de 29.000€/anuales lo que equivale en torno a 12.94€/hora, si hacemos la media entre ambos sueldos para poder obtener un precio/hora aproximado obtenemos que el desarrollador Junior cobrará 12.05€/hora.

En cuanto al salario del tutor del proyecto hemos obtenido la información del sueldo medio consultando diversas páginas de Internet, finalmente, tomaremos para este proyecto la información que proporciona la página web de profesores más popular en España, Superprof [25]. En un artículo se publica que el sueldo medio de un profesor universitario en España es de 53.674€/anuales más luego ingresos que se obtengan por trabajos de investigación, esto equivale aproximadamente a 23.66€/hora.

Se ha realizado una estimación de las horas de trabajo por tarea y del precio de estas que se muestra a continuación:

TABLA 5.2. ESTIMACIÓN DE HORAS Y COSTES DEL PROYECTO

Tareas	Horas	Sueldo/hora	€/tarea
Preparación y Diseño			
Especificación de requisitos	5	23,66 €	118,30 €
Lectura de documentación	20	11,05 €	221,00 €
Formación Desarrollo Aplicaciones web	30	11,05 €	331,50 €
Planificación del proyecto	10	11,05 €	110,50 €
Estudio del proyecto anterior para rediseñarlo	15	11,05 €	165,75 €
Diseño del proyecto (I)	20	11,05 €	221,00 €
Diseño del proyecto (II)	15	11,05 €	165,75 €
Desarrollo			
Desarrollo del código (I)	90	11,05 €	994,50 €
Desarrollo del código (II)	60	11,05 €	663,00 €
Pruebas (I)	20	11,05 €	221,00 €
Pruebas (II)	20	11,05 €	221,00 €
Comprobación de detalles finales previos a entrega	10	11,05 €	110,50 €
Documentación			
Realización de la memoria	120	11,05 €	1.326,00 €
Corrección de la memoria	20	23,66 €	473,20 €
TOTAL			5.343,00 €

Tareas realizadas por	Sandra Sánchez Esperante
	Ana Isabel González-Tablas Ferreres

A continuación, hemos representado un gráfico circular que representa el número de horas totales que se han invertido en Preparación y Diseño, Desarrollo y Documentación. En este podemos apreciar que el tiempo invertido en desarrollo ha sido casi el doble que las horas invertidas en preparación y diseño y documentación, esto es lógico puesto que el desarrollo siempre ocupa un tiempo mayor debido a los numerosos problemas que surgen de la programación de una aplicación.

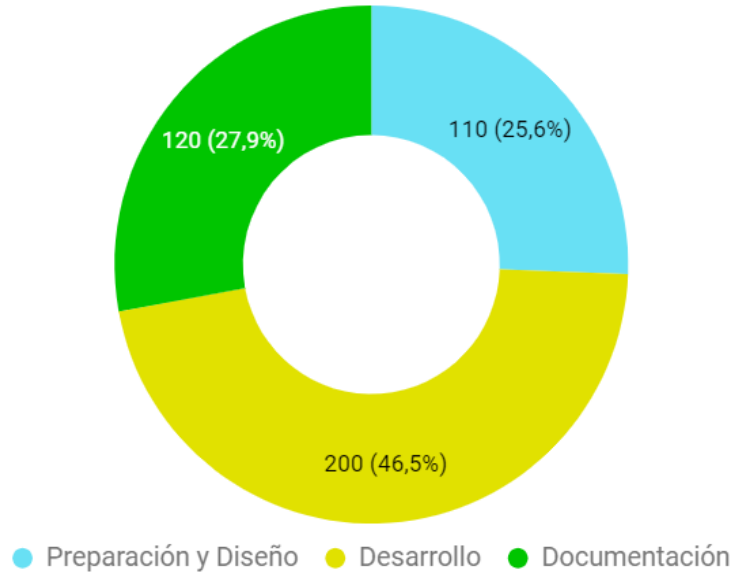


Figura 5.1. Gráfico circular de horas por tareas

6. MARCO REGULADOR

En este capítulo estudiaremos la legislación española y europea actual que debemos tener en cuenta en el momento de publicación de la aplicación web.

6.1. Ley Orgánica de Protección de Datos de Carácter Personal.

Puesto que esta página web va a tratar datos confidenciales de usuarios es importante tener en cuenta la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Esta Ley Orgánica expone en su artículo 1 que "tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar". [26]

Asimismo, cabe destacar el capítulo 4 en el que se defiende la calidad de los datos, y se expone que los datos recogidos únicamente podrán ser tratados para la finalidad con la que fueron recogida. Estos datos no pueden compartirse con terceros ni usarse para otros fines.

"Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos". [26]

6.2. Reglamento europeo de protección de datos.

RGPD es el reglamento europeo de protección de datos, al igual que el documento anterior persigue proporcionar a los ciudadanos una seguridad sobre sus datos confidenciales y castiga a aquellas empresas o usuarios que los vulneren. A diferencia del documento anterior este se amplía a todo el territorio europeo.

Este Reglamento pretende dar mayor poder a los interesados sobre sus datos personales, tanto en redes sociales, smartphones y banca online. [27]

Figura 6.1. Nuevos cambios en la normativa europea y española [27]

6.3. Real Decreto por el que se regulan los certificados de profesionalidad.

El Real Decreto 34/2008, de 18 de enero, por el que se regulan los certificados de profesionalidad se ve complementado con la Ley Orgánica de Protección de Datos de Carácter Personal y defiende la importancia de no vulnerar los derechos de los españoles y su confidencialidad. [28]

6.4. Constitución española.

La Constitución española en su artículo 18 punto 4, establece que se puede limitar el uso de la informática si no se garantiza la seguridad e intimidad de los usuarios.

"4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos." [29]

7. CONCLUSIONES

En este apartado se exponen las conclusiones obtenidas tras la finalización del proyecto. Asimismo, se detallan las futuras líneas de trabajo que optimizarán el proyecto Cybersecurity Sorting Hat.

7.1. Objetivos cumplidos.

Para garantizar si se han cumplido los objetivos propuestos al inicio del proyecto se realiza a continuación una evaluación de cada uno de ellos.

- Remodelar la estructura previa del proyecto anterior para optimizarla. Esta estructura ha sido completamente mejorada, como se ha expuesto anteriormente en esta memoria, se ha rehecho desde cero la estructura de la aplicación para que tenga un código más claro, organizado y sencillo de modificar para futuras mejoras.

- Crear usuarios con sus procesos de autenticación para que la información sólo pueda ser visible por el propio usuario y de esta manera poder proteger la privacidad del usuario y su información confidencial. Efectivamente se ha creado una base de datos donde se guarda la información privada de los usuarios y se ha modificado la aplicación para que tenga un portal de acceso que limite la visibilidad de la información de los usuarios únicamente a estos.

- Diseñar una interfaz de usuario para que sea sencilla e intuitiva para los usuarios y sus respectivas pruebas de User Experience para comprobar que realmente se han cumplido estos objetivos. Hemos podido comprobar a lo largo de esta memoria que se ha modificado la interfaz y se han realizado unas pruebas de UX para comprobar su fácil uso.

- Rediseñar el conjunto de pantallas visibles para el usuario para poder aumentar las funcionalidades de la aplicación. Se ha sustituido el antiguo modelo de una única pantalla que ocultaba y hacía visible los distintos elementos de la

aplicación por una aplicación compuesta de cuatro pantallas: login, about, test y dashboard.

- Incluir dashboards con información del usuario para que pueda observar de una manera clara aquellas áreas que necesita reforzar.

- Incluir procesos seguros de autenticación contra la inyección SQL. Se han revisado diferentes elementos de seguridad, situados entre las vulnerabilidades más habituales.

Inicialmente, se buscaba una aplicación web que completa que cumpliera los requisitos de este TFG y los del otro TFG de nombre análogo. Como se ha mencionado a lo largo de todo el proyecto, el otro TFG no ha podido ser completado a tiempo y se pospone la integración de ambas partes a la fecha en la que la que se finalice el otro Trabajo Fin de Grado.

7.2. Líneas futuras de trabajo.

A medida que se desarrollaba la aplicación web han surgido distintas ideas que podrían ayudar a mejorar el proyecto en un futuro. Algunas de las futuras líneas de trabajo son:

- Ofrecer puestos de trabajo en el ámbito de la ciberseguridad interesantes para los usuarios.
- Ofrecer una pantalla con acceso certificaciones y cursos de utilidad para los usuarios.
- Ofrecer un perfil para las empresas.
- Ofrecer un apartado "¿Olvidaste la contraseña?" y reforzar la seguridad de la opción, puesto que es la segunda vulnerabilidad más habitual.
- Desarrollar la aplicación en entornos Android e iOS para posteriormente publicarla en marketplaces.
- Ampliar los datos de usuario y poder modificar la imagen del usuario.
- Ofrecer una opción para modificar los datos de usuario.

7.3. Conclusiones personales.

La elección de este Trabajo Fin de Grado fue costosa, estuve varios meses en reuniones con distintos profesores para poder ver distintos proyectos y elegir el que encajara más conmigo.

Tenía claro que quería un trabajo que fuera útil, que no se quedara simplemente en un documento que moriría almacenado en la biblioteca, buscaba algo que tuviera algún efecto y fuera relevante en un futuro.

Otro de los aspectos que valoraba en un proyecto es que estuviera relacionado con algo que me apasionara, que pudiera acercarme a cosas que no hubiera visto en la universidad, o que no se hubiera profundizado tanto en ellas.

Cuando fui a ver a mi tutora me relató como un chico del Máster de Ciberseguridad, rama de la carrera profesional que más captaba mi atención, había comenzado una aplicación para estudiantes de este máster pero que, por escasez de tiempo, no había sido capaz de finalizar.

El proyecto captó mi atención en seguida, y decidí aceptar este reto. Una vez finalizado el TFG, afirmo que ha sido una excelente elección. Me ha permitido ayudar y ahorrar costes a la universidad que ha sido como un hogar estos últimos años, y de alguna manera devolver un poco de lo mucho que me ha aportado. He podido ampliar mis conocimientos de desarrollo de aplicaciones web y me ha acercado al mundo de la ciberseguridad que tanto llama mi atención.

ANEXO A: MANUAL DE USUARIO

El presente anexo describe las operaciones y los procedimientos a seguir por los usuarios del Servicio de Cybersecurity Sorting Hat para el correcto uso del mismo.

Registrar usuario

Para registrar un usuario es necesario completar el formulario de Registro, debemos introducir el nombre, email y contraseña. La contraseña pueden ser letras (excluyendo la letra ñ y las tildes) o números.

Acceder a la aplicación

Para acceder a la plataforma es necesario introducir las credenciales y presionar el botón de Login.

Consultar información personal

Las consultas relativas al usuario tales como Nombre, Email, Tipo de usuario podremos encontrarlos en la pantalla About, en la parte inferior del carrusel con imágenes.

Consultar información acerca del Framework

A continuación de la información personal, encontraremos información relativa al marco NCWF. Asimismo, encontraremos una imagen con las 7 categorías que determina el marco.

Realizar el test

Para realizar el test se debe acceder a la pestaña Test. En ella se seleccionarán los TKSA's que posea el usuario. Una vez que se haya completado la selección se hará clic en el botón GO.

Una vez que se haya accionado el botón se mostrará en pantalla el perfil de seguridad de la información que más se acerque al usuario.

Comprobar el perfil de ciberseguridad del usuario

Si el usuario quiere comprobar su perfil, deberá acceder a la pestaña "Dashboard" donde quedará guardado el perfil obtenido en el Test. Si el usuario no ha tomado nunca el test, este apartado mostrará la palabra "Ninguno" a continuación de Perfil del usuario.

Comprobar las debilidades y fortalezas del usuario

Si el usuario quiere comprobar su perfil, deberá acceder a la pestaña "Dashboard". Ahí podrá encontrar diferentes gráficas que muestran las áreas en las que debe mejorar para poder ser un usuario competitivo. En caso de no haber tomado el test previamente esta sección aparecerá con los campos en blanco.

Cerrar sesión

Para cerrar sesión el usuario deberá hacer clic en el botón situado en la parte derecha de la barra de navegación.

ANEXO B: CUESTIONARIOS DE PRUEBAS UX

[30]

1. USUARIO 1

TABLA ANEXO B.1. Usuario 1

¿Cómo se llama?	Usuario1
¿A qué se dedica?	Estudiante Ingeniería Telemática
¿Con la información que se ofrece en pantalla, es posible saber a qué institución o empresa corresponde el sitio? ¿Cómo lo sabe?	Sí, aparece el nombre del Máster y la Universidad en la parte inferior.
¿Relaciona los colores predominantes en el sitio web con la institución?	No, pero está el logo en la barra del buscador con los colores de la universidad.
¿Hacia qué tipo de audiencia cree usted que está dirigido este sitio? ¿Por qué?	Alumnos del Máster
¿Le parece adecuada la selección de contenidos destacados en la portada o usted echó de menos otras áreas de información que le habría gustado ver destacadas?	Si
¿Ha logrado completar exitosamente el proceso para realizar el test?	Si
¿Ha logrado registrarse como usuario?	Si
¿Ha entendido los datos del Dashboard?	Si

2. USUARIO 2

TABLA ANEXO B.2. Usuario 2

¿Cómo se llama?	Usuario2
¿A qué se dedica?	Estudiante Ingeniería Telemática
¿Con la información que se ofrece en pantalla, es posible saber a qué institución o empresa corresponde el sitio? ¿Cómo lo sabe?	Sí, aparece el nombre del Máster y la Universidad en la parte inferior. Además, está el logo en la barra del buscador.
¿Relaciona los colores predominantes en el sitio web con la institución?	No
¿Hacia qué tipo de audiencia cree usted que está dirigido este sitio? ¿Por qué?	Alumnos del Máster
¿Le parece adecuada la selección de contenidos destacados en la portada o usted echó de menos otras áreas de información que le habría gustado ver destacadas?	Si, aunque hubiera detallado más información del marco
¿Ha logrado completar exitosamente el proceso para realizar el test?	Si
¿Ha logrado registrarse como usuario?	Si
¿Ha entendido los datos del Dashboard?	Si, con dudas

3. USUARIO 3

TABLA ANEXO B.3. Usuario 3

¿Cómo se llama?	Usuario3
¿A qué se dedica?	Estudiante Ingeniería Telemática
¿Con la información que se ofrece en pantalla, es posible saber a qué institución o empresa corresponde el sitio? ¿Cómo lo sabe?	Sí, aparece el nombre del Máster y la Universidad en la parte inferior.
¿Relaciona los colores predominantes en el sitio web con la institución?	No, pero está el logo en la barra del buscador
¿Hacia qué tipo de audiencia cree usted que está dirigido este sitio? ¿Por qué?	Alumnos del Máster
¿Le parece adecuada la selección de contenidos destacados en la portada o usted echó de menos otras áreas de información que le habría gustado ver destacadas?	Si, está correcto así, sino se sobrecargaría de información
¿Ha logrado completar exitosamente el proceso para realizar el test?	Si
¿Ha logrado registrarse como usuario?	Si
¿Ha entendido los datos del Dashboard?	Si

4. USUARIO 4

TABLA ANEXO B.4. Usuario 4

¿Cómo se llama?	Usuario4
¿A qué se dedica?	Graduado en Marketing
¿Con la información que se ofrece en pantalla, es posible saber a qué institución o empresa corresponde el sitio? ¿Cómo lo sabe?	Sí, aparece el nombre de Universidad
¿Relaciona los colores predominantes en el sitio web con la institución?	No lo sabe, no está familiarizado con la universidad
¿Hacia qué tipo de audiencia cree usted que está dirigido este sitio? ¿Por qué?	Alumnos del Máster de Ciberseguridad
¿Le parece adecuada la selección de contenidos destacados en la portada o usted echó de menos otras áreas de información que le habría gustado ver destacadas?	Si
¿Ha logrado completar exitosamente el proceso para realizar el test?	Si, aunque al ser un perfil de ciencias sociales no entendía los TKSAs
¿Ha logrado registrarse como usuario?	Si
¿Ha entendido los datos del Dashboard?	Si, con varias dudas

5. USUARIO 5

TABLA ANEXO B.5. Usuario 5

¿Cómo se llama?	Usuario5
¿A qué se dedica?	Estudiante de Ingenieria de Sistemas de Comunicaciones
¿Con la información que se ofrece en pantalla, es posible saber a qué institución o empresa corresponde el sitio? ¿Cómo lo sabe?	Sí, aparece el nombre de Universidad y del Máster. Además está el logo en la barra del buscador.
¿Relaciona los colores predominantes en el sitio web con la institución?	Si
¿Hacia qué tipo de audiencia cree usted que está dirigido este sitio? ¿Por qué?	Alumnos del Máster de Ciberseguridad
¿Le parece adecuada la selección de contenidos destacados en la portada o usted echó de menos otras áreas de información que le habría gustado ver destacadas?	Si
¿Ha logrado completar exitosamente el proceso para realizar el test?	Si
¿Ha logrado registrarse como usuario?	Si
¿Ha entendido los datos del Dashboard?	Si

ANEXO C: ENGLISH VERSION

ABSTRACT

This document aims to detail the functionalities of the Cybersecurity Sorting Hat project. This project is a Web application, initially destined to the students of the Master's Degree in Cybersecurity of the University Carlos III, but that can be modified to be of utility to all the users interested in this field.

Originally, the project emerged from the need to classify information security professionals in very well defined frameworks, which is why the most popular framework known by the NICE Cybersecurity Workforce Framework was taken as a reference.

The main functionality of the application is to be able to determine the profile, in terms of cybersecurity roles, of these professionals.

This end-of-degree work consists of the continuation, modification and improvement of an end-of-master's work carried out by a colleague from Carlos III University.

The previous project has been redone from scratch in many aspects, such as user interface or code structure, also it was necessary to modify databases so the previous design has played a fundamental role since it has had two roles not only to organize the new structures, but it has also been vital to be able to adapt and modify the previous project.

This document details the stages of planning, design, development, and documentation that have been carried out during the project, also explains the functionalities that have been developed and the relevance that these have for the correct functioning of the application.

PREVIOUS NOTES ON THE WORK

Before reading the project, it is necessary to explain the background of it. The end-of-degree work is the continuation and improvement of an end-of-master work of a colleague of the Carlos III University, Javier Vila, titled "Cyber Range Systems: A Cybersecurity Sorting Hat".

This is a large web application that could not be completed in a single TFM, and it is continued and improved in this end-of-degree work.

The client had many ideas to complete this project. In order to fulfil all the client requirements two students have continued the project, Javier Sanz López and Sandra Sánchez Esperante.

We have both developed different functionalities, but we share the same nucleus and the end-of-degree works complement each other. This complementarity will therefore be reflected in the memoirs.

1. INTRODUCTION

This chapter makes a brief introduction of the project and details the motivation that it has led to doing it. The main objectives and functionalities that will be developed are also exposed. Finally, the structure that follows the project is detailed.

1.1. Aim of the work.

Today's society is a hyperconnected society. The Internet of Things (IoT) has facilitated the connection of objects that a few years ago could not have imagined that they could access the Internet.

This connection of everything around us, from working life to staff, makes it necessary to implement techniques to protect our security.

In 2017 we saw a massive increase of cyberattacks [1], these were not only operations of ransomware against companies, but we also lived attacks defended by states, leaks of state documents and hackings of electoral campaigns. The most popular were the Vault7 filtration of Wikileaks and the ransomware WannaCry.

Only Spain recorded more than 120,000 cyber-attacks last year according to INCIBE (National Cybersecurity Institute of Spain). This figure has increased by 140% in two years [2].

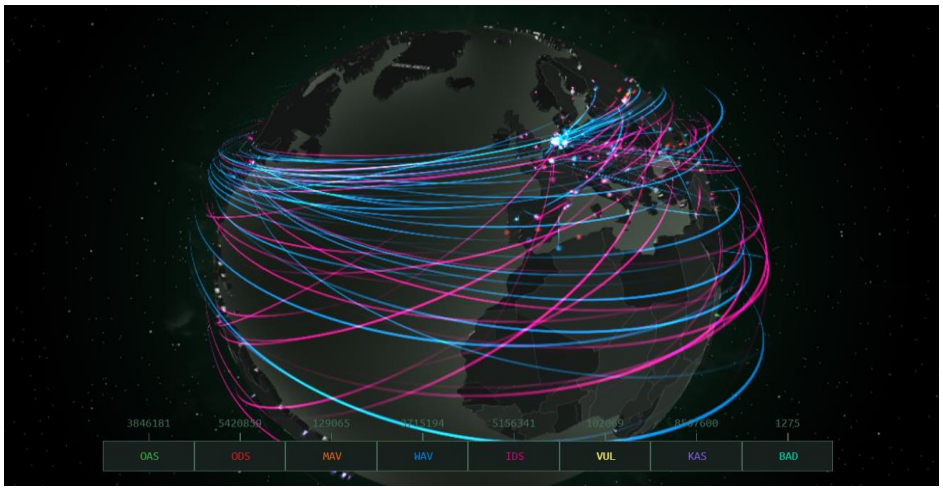


Figure C.1. Capture that allows to see cyberthreats in real time [3]

Because of this massive increase in attacks, it is becoming more and more necessary to train professionals in this sector. The World Center for Cyber Security and Education

(ISC) states in its Global Information Security Study (GISWS) that 66% of security companies do not have enough employees to cope with all threats. It is expected that security departments will expand by more than 20% in the next year, which is equivalent to 1.8 million more workers to cover those vacancies [4].

Companies, in the hope of covering these vacancies, look for very specific profiles. The purpose of this project is to help students determine what profile they meet or what characteristics or requirements are sought for a specific profile, and thus be able to increase their employability ratios.

It is also an useful tool for companies that would like to see what characteristics their employees should meet.

The classification of profiles that we are going to follow is the organization proposed by in NICE Cybersecurity Workforce Framework (NCWF) [5]. This classification consists of 7 categories that group common functions, 33 areas of expertise and 52 work papers that in turn comprise the knowledge and skills needed to perform those positions.

1.2. Objectives.

The end-of-degree work aims to help professionals in the cybersecurity sector discover their profile and improve the skills that they need to become competitive professionals in the labour market. Although users are professionals in the IT sector, it is important to develop a simple and easy-to-use application.

Taking into account the requirements we can define the main objective is to allow the user to define his profile in the computer security sector and give him tools to achieve it.

To achieve this purpose, it is necessary to:

- Remodel the previous structure of the earlier project to optimize it.
- Create users with their authentication processes so that the information can only be visible by the user itself and in this way be able to protect the user's privacy and confidential information.

- Design a user interface simple and intuitive for users and their respective User Experience tests to verify that these objectives have really been fulfilled.
- Redesign the set of screens to be able to increase the functionalities of the application.
- Include dashboards with user information so they can clearly observe the areas needed to reinforce.
- Include secure authentication processes against SQL injection.

1.3. Structure of the document.

This section describes in a general way the structure of the document.

- Introduction and Objectives: This chapter deals with the current situation, the problem that exists in the cybersecurity sector due to the lack of professional profiles and the numerous cyberattacks that occur daily. Therefore, the need of an application that helps the professionals to determine their profile and what are their weaknesses and strengths is exposed.

- State of art: This chapter focuses on reviewing the technical aspects of the current situation. It describes similar applications that exist in other nations and performs a comparison of functionalities with the application that is going to be developed in this project. It also sets out the profile frameworks of cybersecurity professionals and the reasons for the choice of the NICE Cybersecurity Workforce Framework.

- Design and Software Development: This chapter analyses and describes the design of the technical solution. Detailed developments that have been made to achieve a simple and useful application. It deals with all aspects of the modifications that have been developed from a technical point of view.

- Planning and Budgeting: This chapter shows the previous planning that has been made of the project. It also details the estimated project budget. This is an important chapter since it shows both time management and resources.

- Regulatory framework: A study of current Spanish and European legislation that will affect the publication of the web application.

- Conclusions: This chapter outlines the conclusions that have been extracted from the end-of-degree work. We will review the fulfilment of the objectives proposed at the beginning of the project and propose some future lines of the project.

2. STATE OF ART (SUMMARY)

Nowadays, the search for cybersecurity profiles is a priority subject for companies, we can find some pages online that perform a similar function to this project, but none is completely the same.

An analysis of the current competition has been carried out in order to find the differential aspects of our application, and then the main characteristics of this competence are detailed. We must add that the applications mentioned below are aimed at developing the professional career in the United States. Therefore, we can conclude that there is no similar application to this project in the Spanish market.

National Initiative for Cybersecurity Careers and Studies (NICCS) [6] is a U.S. government-owned Web application belonging to Homeland Security, which connects government employees, students, and teachers to cybersecurity training providers.

NICCS's vision is to provide the tools and resources needed to ensure that workers in cybersecurity have adequate training and education. Its mission is to be a resource for education, careers and training in cybersecurity.

CyberDegrees.org was created by Degree Prospects, a Washington, DC-based publisher of informational websites in higher education.

There is functionality in this web that is related to our project. It's called "Career Path". In this section we can find different professional positions of computer security. If we click on each one of them they will provide information about the job.

Institute of Information Security Professionals (IISP) is an independent, non-profit organization governed by its members. It is headquartered in London and was created in 2006 by professionals in the field of cybersecurity [10].

Its website offers functionalities similar to the ones in this project. Not only the user can verify what IT security profile he has, but also we can find other features such as the offer of jobs related to profiles in information security.

It is also important to mention that there are different frameworks that organize the skills. For this Project the NCWF was selected but we must explain the differences and similitudes between the most important frameworks.

NICE Cybersecurity Workforce Framework (NCWF) is the most widely used framework [5], it is used in the vast majority of the web applications described below. It is a special publication of NIST with global alignment that categorizes and describes the various positions in cybersecurity based on TKSAs.

U.S. Coast Guard Cybersecurity Framework Profile for offshore operations is a framework defined by the U.S. government's offshore operations the U.S. Coast Guard (USCG) in collaboration with the National Institute of standards and Technology (NIST) Cybersecurity Center of Excellence (NCCoE) [12].

This framework modifies the NCWF framework to be oriented to the fields of missions in the American army. It is therefore a modification of the NCWF.

Financial Services Sector Specific Cybersecurity profile ("Profile") as the previous framework, it is a framework that comes from a modification of the NCWF that incorporates aspects of American regulation. It is oriented to the security of the information in financial sectors [14].

Now that we have seen the most relevant solutions worldwide we can conclude that the solution proposed for this project consists in the development of a web application with unique features in the Spanish territory similar to the ones in other countries.

It is a leading application in the field of information security and benefits for both students and companies.

This solution, as previously mentioned, is based on the NCWF framework. We have chosen this framework as the optimal option because it is the most common and popular categorization of profiles in the cybersecurity sector.

This choice allows the user's radius to be greater and, in the long run, users not belonging to the Carlos III University can use it.

3. ANALYSIS AND DESIGN (SUMMARY)

This chapter provides an analysis of the technical solution and describes the architecture proposed for the application. The project requirements and use cases are then exposed.

A layer architecture has been made.

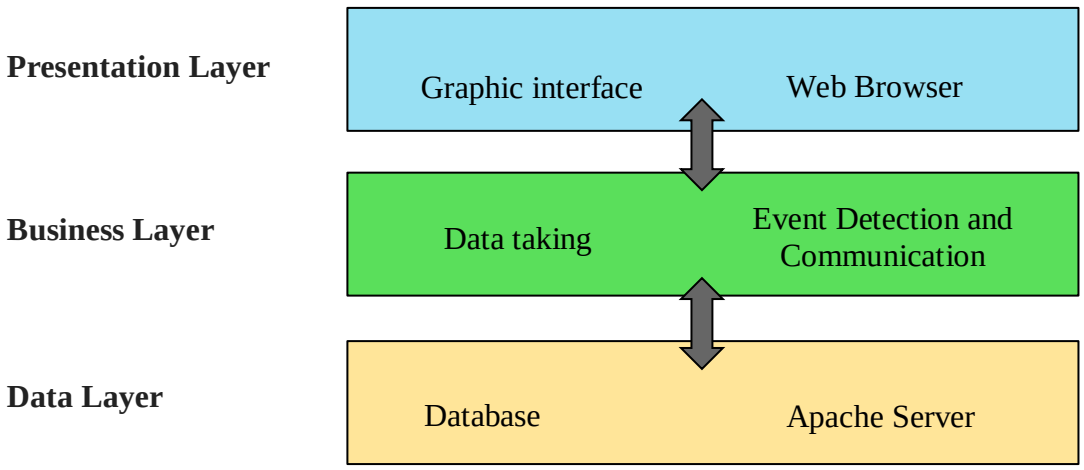


Figure C.2. App architecture

The Software Requirements Specification (ERS) is a description of the ideal behaviour that the system should have. [17] We can differentiate between functional and non-functional requirements.

Functional Requirements

- RF01 User Register.
- RF02 User Authentication.
- RF03 Logout.
- RF04 Taking the test.
- RF05 Sending the test.
- RF06 Modify the test.
- RF07 Check the dashboard.

Non Functional Requirements

- RF08 Internet conection.
- RF09 Protect the data.
- RF10 Developement in PHP.

Use cases are descriptions of the activities that need to be done to carry out a process. This is the sequence of interactions that develop between a system and its actors. There is a use case drawn in the Spanish part for each Functional Requirement.

4. SOFTWARE DEVELOPEMENT (SUMMARY)

The previous design to the development of the application has been vital for reaching the agreement between the requirements and the final result of the project.

This project is part of a previous project, that not only has it been necessary to continue, but it was also necessary to make improvements and modifications to optimize the solution.

The application has been developed in HTML. It has maintained the PHP programming language in which the previous version was developed and was used to access the databases.

The application has been developed in PHP, HTML, JS and CSS. PHP has been used in relation to the database connection and the application exchanges with it. HTML to make a web application in a structured way. CSS has been used to obtain a visually appealing interface. JS for the detection and communication of events.

An "Agile" methodology has been used since the project required fast collaboration between the two students. Weekly meetings have been held to check the progress of the team and to verify that the objectives were being fulfilled.

Below we can find the flowchart of the entire project, these are the steps that the user will have to follow when he wants to use the application. This diagram does not include the registration.

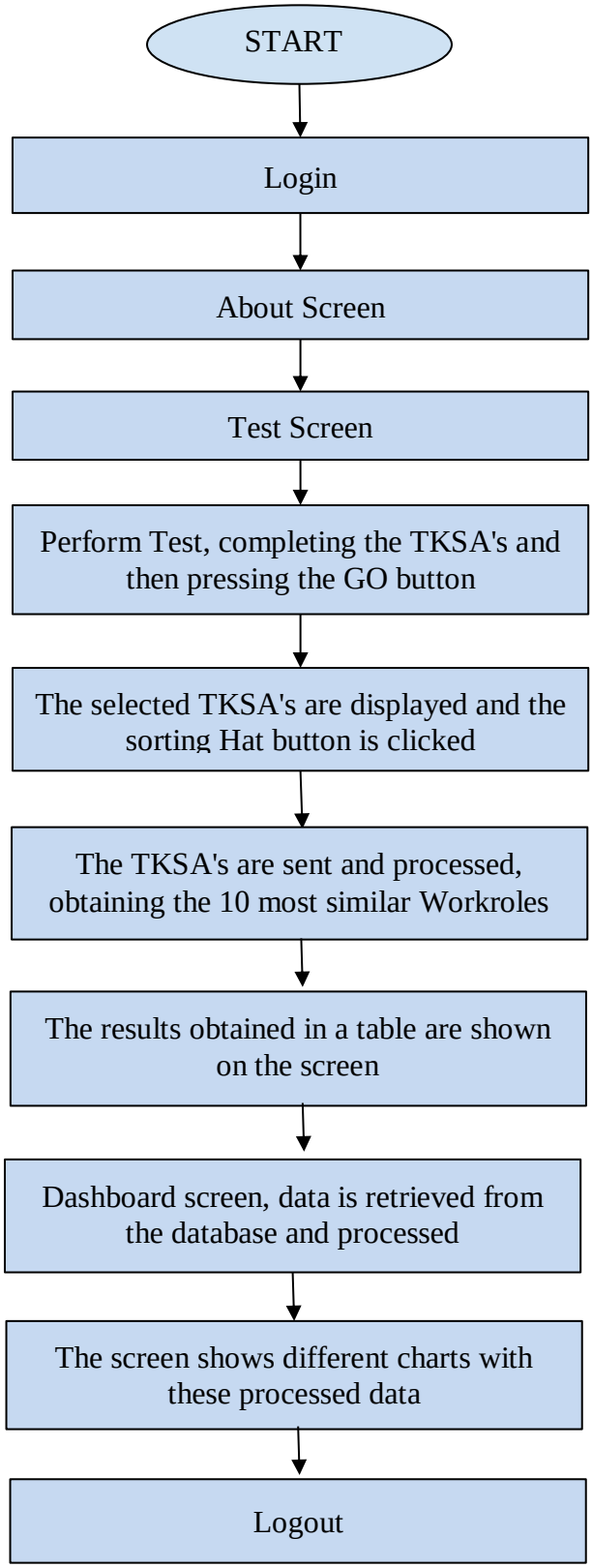


Figure C.3. Flowchart

The developer who made the first version of the project made an application design that consisted in implementing the entire web application on a single screen and showing or hiding the elements depending on the state of the process in which we were.

If the user was making the selection of TKSAs, the web application made visible only the elements related to this step and kept hidden the rest of elements.

In the design of this project we have decided to improve this structure and we have created different pages that coincide with the different steps that a user will make. We have erased all that code related to these processes and we have redesigned and recoded the application.

The purpose of this change is to provide a clearer and more intuitive development. It is necessary to add, that modifying the previous structure facilitate the increase of functionalities of the system. The development of future functionalities will only be influenced by the development itself and not by the concern to hide elements of old functions.

To be able to develop the web application, the programmers have installed the XAMPP program for Windows.

The graphical interface of the application has been redesigned and has been programmed from scratch in order to obtain a clear, simple and attractive interface for the user. For the application to be visually more appealing to the user, Bootstrap has been employed.

The application consists of four screens.

The first screen is the Login Screen, it is the page in which users can access the system, register or send an email in case they have forgotten the password.

The second screen is the About Screen; this is the service presentation page. In this section we can find a navigation bar that redirects us to the next two screens. We will look at a carousel with images and phrases related to information security. We can also

find a description of the user profile. Finally, we will find a description of the service and information related to the NICE Framework that is used for the categorization of profiles.

The third screen is the Test Screen, in this screen the user will enter the KSA's that he has and then press the Test button. Once the user presses this button the comparison and analysis of the similarities with the profiles of the NICE Framework will be made. After this comparison the application will show the results of the evaluation and assign the user the profiles that most fit with their skills and knowledge.

The fourth and last screen is the Dashboard Screen, this screen shows user-related graphics. It facilitates the visualization of the strengths and points to be improved by the user.

An User Experience interview has been made to a sample of 5 students of the university Carlos III. UX interviews consist of recording screen and audio and asking users for different tasks that are related to the Web application to see if they manage to perform the actions without problems or if the interface is not intuitive and it is too complex to finish the professional profile search process. These interviews demonstrate that the graphic interface is easy to use and attractive to the users.

In terms of security, OWASP's TOP 10 vulnerabilities has been reviewed and the following solutions have been taken.

To protect from the SQL injection, we have separated the sensitive data of the user from the query that is done to the database. In the case of the code of this application we can see protection against injection in processes such as user authentication or registration of this.

The database has been protected with user and password that only the developers know of this project, in this way, we prevent that any user of the application can access the database and manipulate it.

To protect the application, the parameters that are used for the connection have been extracted from PHP and moved to another document in another folder.

```
require "../connect.inc.php";
$enlace = new mysqli($Host, $User, $Password, $DBName);
```

5. PLANNING AND BUDGETING (SUMMARY)

The development of the project has lasted four months. It has followed a proposed planning at the beginning of this since it was necessary the coordination of two developers.

To perform this planning a GANTT chart has been developed with the functions that have been performed in this project and the duration of these

The project has not needed a CAPEX investment in physical infrastructure or material goods. This is a software project so the costs come directly from the cost of the hours that have been used by the members of this.

For the development of the project a Junior programmer has been chosen, this benefits the client because it reduces the costs compared to hiring a Senior developer.

6. REGULATORY FRAMEWORK (SUMMARY)

In this chapter we study the current Spanish and European legislation that we must take into account at the time of publication of the web application.

Since this website will address confidential user data it is important to take into account the Organic law 15/1999, of 13 December, on personal data protection.

RGPD is the European Data Protection regulation, just as the previous document aims to provide citizens with security over their confidential data and punishes those companies or users that violate it. Unlike the previous document, it is extended to the entire European territory.

The royal Decree 34/2008, of 18 January, by which regulate the certificates of professionalism is complemented with the Organic Law of protection of personal data and defends the importance of not violating the rights of the Spaniards and their confidentiality.

The Spanish Constitution in article 18, point 4, states that it is possible to limit the use of computers if the security and privacy of the users are not guaranteed.

7. CONCLUSIONS

This section sets out the conclusions obtained after the completion of the project. It also details the future lines of work that will optimize the Cybersecurity Sorting Hat project.

7.1. Fulfilled objectives.

In order to ensure that the proposed objectives have been fulfilled at the beginning of the project, an evaluation of each one of them is carried out.

- Remodel the previous structure of the earlier project to optimize it. This structure has been completely improved, as previously stated in this memory, the structure of the application has been remade from scratch so that it has a clearer, organized and easy to modify code for future improvements.

- Create users with their authentication processes so that the information can only be visible by the user itself and in this way be able to protect the user's privacy and confidential information. Indeed, a database has been created where users ' private information is stored and the application has been modified so that it has an access portal that limits the visibility of users ' information only to these.

- Design a user interface to make it simple and intuitive for users and their respective User Experience tests to verify that these objectives have really been fulfilled. We have been able to verify throughout this memory that the interface has been modified and UX tests have been performed to verify its easy use.

- Redesign the set of screens visible to the user to be able to increase the functionality of the application. It has replaced the old model of a single screen that hid and made visible the various elements of the application by an application composed of four screens: login, about, test and dashboard.

- Include dashboards with user information so you can clearly observe those areas you need to reinforce.

- Include secure authentication processes against SQL injection. Different security features have been reviewed, located among the most common vulnerabilities.

7.2. Future lines of work.

As the web application was developed, different ideas emerged that could help improve the project in the future. Some of this future lines of work are:

- Provide jobs in the field of cybersecurity that are interesting for users.
- Offer a screen with access certifications and useful courses for users.
- Offer a profile for companies.
- Offer a section "Forgot your password?" and reinforce the security of the option, since it is the second most common vulnerability.
- Develop the application in Android and IOS environments to later publish it in marketplaces.
- Expand user data and be able to modify the user's image.
- Offer an option to modify user data.

7.3. Personal conclusions.

The choice of this end of grade work was expensive, I spent several months in meetings with different teachers to see different projects and choose the one that fit more with me.

I wanted a job that was useful. I did not just stay in a document that would die stored in the library. I was looking for something that had some effect and was relevant in the future.

Another aspect that I valued in a project is that it was related to something that I was passionate about, that I could learn things that I had not seen in university, or that had not learnt in depth.

When I went to see my tutor she told me about the project of a student of the Master's Degree in Cybersecurity, branch of the professional career that most caught my attention. This student had started an application for students of this Master's but he had not been able to finish it.

The project caught my attention at once, and I decided to accept this challenge. Once the TFG is finished, I affirm that it has been an excellent choice. It has allowed me to help and save costs to the university that has been like a home this last years, and somehow give back a little of how much it has taught me. I have been able to expand my knowledge of web application development and it has brought me closer to the world of cybersecurity that draws my attention.

BIBLIOGRAFÍA

[1] Los mayores ciberataques de 2017 hasta la fecha, 07-2017 [En línea] Disponible en: https://www.pandasecurity.com/spain/mediacenter/noticias/ciberataques-hasta-la-fecha/

[2] España bate su récord en ciberataques: 120.000 incidentes en 2017, 12-01-2018 [En línea] Disponible en: http://www.abc.es/tecnologia/informatica/abci-espana-bate-record-ciberataques-120000-incidentes-2017-201801111645_noticia.html

[3] Imagen de ciberataques en tiempo real, Kapersky [En línea] Disponible en: https://www.cybermap.kaspersky.com/es/

[4] 2 millones de trabajadores en ciberseguridad para 2022, Miriam Martínez, 30-11-2017 [En línea] Disponible en: https://www.cice.es/noticia/necesidad-trabajadores-en-ciberseguridad/

[5] NICE Cybersecurity Workforce Framework, 20-02-2018 [En línea] Disponible en: https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

[6] About NICCS, 21-06-2017 [En línea] Disponible en: https://niccs.us-cert.gov/about-niccs

[7] Mapping Tool, 02-03-2018 [En línea] Disponible en: https://niccs.us-cert.gov/workforce-development/intro-mapping-tool

[8] PushButtonPD, 29-03-2018 [En línea] Disponible en: https://niccs.us-cert.gov/workforce-development/dhs-pushbuttonpd-tool

[9] About Cyber Degrees [En línea] Disponible en: https://www.cyberdegrees.org/

[10] IISP: Our Mission [En línea] Disponible en: https://www.iisp.org/imis15/iisp/About_Us/Our_Mission/iispv2/About_us/Our_Mission.aspx?hkey=9a43cc5c-8b71-4770-bfa9-d60e5c7b3ba9

[11] IISP Knowledge Framework - Version 1 [En línea] Disponible en: https://www.iisp.org/imis15/iisp/About_Us/Our_Frameworks/Our_Knowledge_Framework/iisp/About_Us/Our_Knowledge_Framework.aspx?hkey=6e8644f9-fc2f-4f53-9784-b0fb2dba5e8b

[12] National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, NIST, 08-2017 [En línea] Disponible en: https://csrc.nist.gov/csrc/media/publications/sp/800-181/archive/2016-11-02/documents/sp800_181_draft.pdf

[13] U.S. Coast Guard Cybersecurity Framework Profile for Offshore Operations, 05-2017 [En línea] Disponible en: https://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/Content%20Preview%20of%20Offshore%20Profile.pdf?ver=2017-07-19-070239-550

[14] Draft Financial Services Sector Specific Cybersecurity Profile [En línea] Disponible en: http://www.fsroundtable.org/bits/draft-fs-cybersecurity-profile/

[15] Financial Services Sector Coordinating Council, Financial Services Sector Specific Cybersecurity "Profile", 17-05-2017 [En línea] Disponible en: https://www.nist.gov/sites/default/files/documents/2017/05/18/financial_services_csf.pdf

[16] Programación por capas, Wikipedia, 11-04-2018 [En línea] Disponible en: https://es.wikipedia.org/wiki/Programaci%C3%B3n_por_capas

[17] Especificación de requisitos de software, Wikipedia, 07-02-2018 [En línea] Disponible en: https://es.wikipedia.org/wiki/Especificaci%C3%B3n_de_requisitos_de_software

[18] Casos de uso, Wikipedia, 12-04-2018 [En línea] Disponible en: https://es.wikipedia.org/wiki/Caso_de_uso

[19] NetSuite Solution Provider, Mediante nuestra metodología AGILE ejecutamos con éxito el proyecto, [En línea] Disponible en: http://www.smartstrategyonline.com/site/es/nuestros-socios/netsuite.html

[20] ¿Qué es XAMPP? [En línea] Disponible en: https://www.apachefriends.org/es/index.html

[21] About Bootstrap [En línea] Disponible en: https://getbootstrap.com/

[22] Top 10 2013-Top 10, OWASP Foundation, 2012-2013 [En línea] Disponible en: https://www.owasp.org/index.php/Top_10_2013-Top_10

[23] About OWASP, OWASP Foundation, 22-01-2018 [En línea] Disponible en: https://www.owasp.org/index.php/Main_Page

[24] HAYS Recruiting experts worldwide, Calculadora Salarial [En línea] Disponible en: http://guiasalarial.hays.es/trabajador/calculadora

[25] Marisol, ¿Cuál es el salario de un profesor en España?, 13-09-2017 [En línea] Disponible en: https://www.superprof.es/blog/sueldo-de-un-profesor-en-espana/

[26] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, BOE, 05-03-2011 [En línea] Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/2014/Ley_Organica_15-1999_de_13_de_diciembre_de_Proteccion_de_Datos_Consolidado.pdf

[27] Nueva Ley de Protección de Datos europea ¿qué cambia?, 20-12-2017 [En línea] Disponible en: https://www.protecciondatos-lopd.com/empresas/nueva-ley-proteccion-datos-2018/

[28] Real Decreto 34/2008, de 18 de enero, por el que se regulan los certificados de profesionalidad, BOE, 21-03-2013 [En línea] Disponible en: https://www.boe.es/buscar/pdf/2008/BOE-A-2008-1628-consolidado.pdf

[29] Constitución Española, Cortes Generales, 27-09-2011 [En línea] Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/Constitucion_es.pdf

[30] Modelo de Test de Usuario http://www.guiadigital.gob.cl/guia-v2/capitulos/05/anexos/pauta-test-usuario.pdf